Universiteit Leiden

ICT in Business and the Public Sector

A process approach towards GDPR and PSD2 compliance
for Banking Organizations in the Netherlands

Name:	Tsingani Pinelopi-Apostolia
Student-no:	s1499289

Date:15/07/2022

1st supervisor: Niels van Weeren

2nd supervisor: Bas Kruiswijk

MASTER'S THESIS

Leiden Institute of Advanced Computer Science (LIACS)

Leiden University

Niels Bohrweg 1

2333 CA Leiden

Abstract

The purpose of this study is to investigate how the Banking Organizations have been affected by privacy data regulations published the last three years, GDPR for personal data and PSD2 for transactional. Considering the content of the publications and the new requirements that they were bringing, the focus of this thesis will be on how the organizations have to adapt new principles and ways of working and especially how those are implemented through, not only technology wise but always taking into account the regulatory and supervisory obligations.

The approach followed was a combination of literature review at the first stage and after enriched by two rounds of semi-structured interview rounds as well as an online survey. The research question set were:

Main Question: How the data landscape needs to be reformed in financial services organizations in order to comply with the new regulations of GDPR and PSD2?

Sub-question 1: What are the changes that the new regulations brought to the bank organizations?

Sub-question 2: What actions have been taken so far in the way the financial services organizations manage their data in order to comply with GDPR and PSD2?

Sub-question 3: What are the requirements to be fulfilled in order the financial services organizations to comply with GDPR & PSD2?

The outcome of this study is giving two process flows, one for GDPR and PSD2, with all the requirements identified through our research as mandatory (regulatory obligations) as well as some best or preferred practices that banking organizations have implemented in order to enrich and reassure their compliance to the regulations.

Acknowledgements

First of all, I would like to express my gratitude to my supervisors, Niels van Weeren and Bas Kruiswijk, for all their support, patience, guidance and feedback through this lengthy process. Their contribution was key not only for academic and expertise matters, but also to morally support me and keep me motivated.

In addition, I would like to thank all the participants in the interviews and the online survey. Their participation to my research was crucial for the conduct of this research study, without them I could not collect all this information.

Lastly, I would like to thank my friends and family for being always there for me and supporting me.

Contents

List of figures

List of tables

Thesis title “A process approach towards GDPR and PSD2 compliance for Banking Organizations in the Netherlands”.

1. Introduction

1.1 Background and Problem Statement

Traditionally, financial services organizations have to manage sensitive information of their customers. A lot of attention has been raised the last couple of years because of the new European laws and every financial organization in the Netherlands must comply with them, as well as any other organization doing business in the European Union or with EU residents. Nevertheless, financial organizations are uniquely positioned to comply with GDPR and PSD2 because they have been already subject to some global privacy regulations [6]. The most significant effects appear to be related to the controls that should be applied in order to protect client data. Their processes of managing personal data should be adjusted in order to incorporate the client consent mechanism prior to the collection and assessment of the data [6].

Therefore, not only technology is crucial for data protection, but also the process of managing the information flow to clients, vendors and third parties needs to be carefully adjusted and monitored. The successful combination of IT and process controls would set a solid foundation for data privacy and protection.

Financial services business can vary to different sub-sectors, hence the impact of data privacy regulations can vary also depending on the nature of the business. Retail banks and Insurance companies traditionally keep data for longer periods since it is required for risk model calculations and provisions. However, on investment management business, the focus lies on Business-2-Business (B2B) and there is no need to store personal data [7].

Both GDPR and PSD2 require the businesses to be compliant on aspects in regards to the data collection, the reason of collection, the purpose and the manner they are using it. In order to achieve the required level of compliance, financial organizations need to adjust their processes, means of technology as well as train their employees accordingly. The personal data landscape is moving to a new era and it is rather unavoidable to transform and comply with its requirements.

The purpose of this study is to investigate which new requirements the regulations of GDPR and PSD2 had brought for Financial Institutions, what are the challenges and the restrictions around them and how any new concepts could be implemented or existing IT solutions have been impacted. It is important to capture the current situation, identifying the progress done so far as well as the impediments that can hurdle the implementation of relevant actions. Those aspects can be spotted in different dimensions among an organization; the current study will focus on the process transition in relation with the technology change and the culture, in terms of education and trainings. In particular, we will investigate how financial services companies can move from the traditional way of storing, processing and accessing data to new or updated IT solutions but always in combination with the organizational behaviour; how the employees react to the new data regulations, how willing they are to adjust and get the relevant trainings.

The scope of this study will focus on banking organizations such as Banks in the Retail and Wholesale domains in the Netherlands. At this point it is important to mention that the research will be extended to legal and compliance requirements in order to support the review of the regulations as well as findings and gaps between the new regulations and their predecessors.

1.2 Research Questions

Below there are stated the main research question and the sub-questions that we will try to answer on our research.

Main Question: How the data landscape needs to be reformed in financial services organizations in order to comply with the new regulations of GDPR and PSD2?

Sub-question 1: What are the changes that the new regulations brought to the bank organizations?

Sub-question 2: What actions have been taken so far in the way the financial services organizations manage their data in order to comply with GDPR and PSD2?

Sub-question 3: What are the requirements to be fulfilled in order the financial services organizations to comply with GDPR & PSD2?

2. Methodology

2.1 Research Methodology

In order to answer the research questions, it is important to review all the relevant documentation of GDPR and PSD2. For that purpose it is necessary to develop a good understanding of the new personal data regulations, what differentiate those from past regulations and which are the most crucial sections that would have impact on implementing them within banking services environment.

The most applicable method for our subject, is the *critical review of the literature* since it provides the foundation on which our research will be built [1]. This method focuses on diving into the specific subject and having a detailed examination of the literature, in order to be able to gain an up-to-date insight of the subject but also aim to compare and evaluate different aspects. Table 1 below, summarizes the key points of this critical review method. The nature of this study requires critical evaluation of existing sources as well as the need to be able to retrieve information from a representative sample of articles etc. The critical review strategy needs to be planned in a structural way considering the research objectives, the search criteria and the available sources.

Next to the literature review a qualitative analysis is required in order to examine whether observations from the literature review could be identified in current real-world financial business, spot any related gaps and therefore investigate in depth the new concepts, if any, as well as their integration to the existing organization context (process and people wise) [11]. Furthermore, data collection is required, mainly from interviews and/or questionnaires, and detailed analysis of it in order to evaluate the implementation of the new IT concepts and gain more insight on how the employees have been prepared and trained towards any new or upgraded solution while integrating in the current organization processes.

Overarching goal	**Search strategy**	**Appraisal of included studies**	**Analysis and synthesis**
Aims to provide a critical evaluation and interpretive analysis of existing literature on a particular topic of interest to reveal strengths, weaknesses, contradictions, controversies, inconsistencies, and/or other important issues with respect to theories, hypotheses, research methods or results.	Seeks to identify a representative number of articles that make the sample illustrative of the larger group of works in the field of study. May or may not include comprehensive searching.	No formal quality or risk of bias assessment of included primary studies is required	Can apply a variety of analysis methods that can be grouped as either positivist (e.g., content analysis and frequencies) or interpretivist (e.g., meta-ethnography, critical interpretive synthesis) according to the authors' epistemological positions.

Table 1 Typology of Literature Reviews (adapted from Paré et al., 2015)

2.2 Research Objectives

By setting the research objectives we need to answer two important questions:

1. What are we aiming to achieve by this research?

The reason behind our research is to thoroughly review the relevant regulation documentation as it is published by the formal authorities and get fully acquainted with the subject in terms of content and timeliness. In addition to that, reading relevant papers and supporting articles will help to understand how the way of managing personal data in the financial sector has changed over the past few years, after the new data privacy regulations (define the current situation) and assess the current maturity in comparison with the final target (define target situation). The capture of the transition from the current to target situation includes not only the investigation of new IT concepts that have been introduced but also the relevant impact on the current IT solutions, the internal processes of managing data and the people involved in related activities.

2. How are we going to conduct our research?

Before starting with the search, it is helpful to agree on some key aspects that will smoothen the research phase. The most important ones are:

- To define key search parameters as search domain and rules

Since our research scope is limited to the banking sector, the business sector parameters while searching will be related to sources about *financial institutions*, *banking organizations*, *retail banking, wholesale banking* in relation with the personal data regulations *GDPR* and *PSD2*.

Our aim while searching is not to analyse in detail the full regulations documentation, but to get an insight on what the new articles are adding in existing theory but also analyse further what would be the deviation from the current situation and the impact on the banking services organizations.

The table below presents the key word combination to be used while searching on online sources. In any search combination both AND and OR operators are applicable.

Financial Service Sector **Personal** **Data Regulation**	**Banking Organizations** Banks Retail Banks Wholesale Banking
GDPR	AND/OR
PSD 2	AND/OR

Table 2 Key search word matrix.

The search above can be enriched with two more dimensions related to the business aspects that we would like to focus and emphasize;

-Information Technology (IT): IT concepts that either they have been introduced and implemented and the way there were integrated, or existing IT concepts and the way there were adjusted to fit the new requirements.

-Organizational behaviour: Employees’ reaction in regards to the changes that regulations brought, primary and continuous education on the topics.

- To define the sources that are going to be used as primary and secondary sources for research

The primary literature sources are the first occurrence of a piece of work/documentation [1]. For our review, our sources are the regulations, officially published by EU authorities. In particular as Regulation (EU) 2016/679 (General Data Protection Regulation) and Directive (EU) 2015/2366 (Payment services PSD 2). Typically, these publications are defining the whole scope of their applicability as well as main articles which bring all the relevant information for principles and guidelines imposed by laws.

The nature of our research requires secondary literature sources such as university papers and publications where the regulations are analysed in detail, the changes from older laws are highlighted and potential solutions or approaches are introduced. In the market, there are also publications, provided mainly from consultancy organizations that are active in multiple sectors and focus on services to guide clients through the data regulation law transitions. This kind of white papers, which are publicly available online, can be used as complimentary to the other sources, since they are providing more practical insight and they strongly facilitate the professional needs that the organizations have to fulfil [3]. Therefore they will be important for our search since they can provide some insight on the maturity of the current situation, more than 3 years after the application of the regulations as well as any gaps on market level.

2.3 Plan of Approach

The flowchart below (Figure 1) shows the process of formulating the plan for the current research assessment.

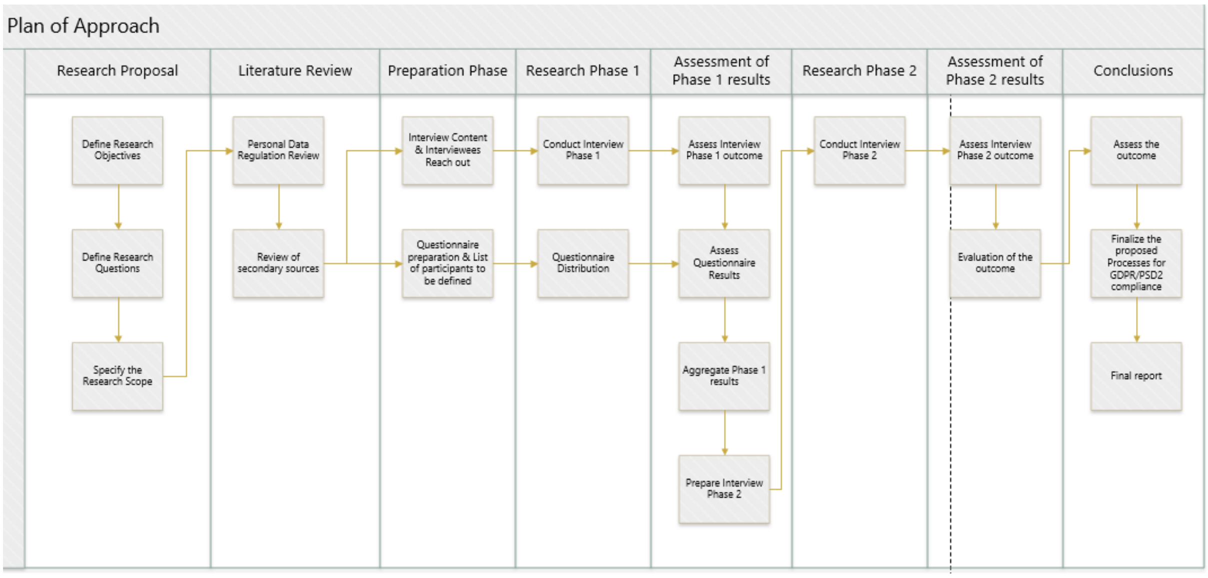

Plan of Approach
Research Proposal
Literature Review
Preparation Phase
Research Phase 1
Assessment of Phase 1 results
Research Phase 2
Assessment of Phase 2 results
Conclusions
Define Research Objectives
Define Research Questions
Specify the Research Scope
Personal Data Regulation Review
Review of secondary sources
Interview Content & Interviewees Reach out
Questionnaire preparation & List of participants to be defined
Conduct Interview Phase 1
Questionnaire Distribution
Assess Interview Phase 1 outcome
Assess Questionnaire Results
Aggregate Phase 1 results
Prepare Interview Phase 2
Conduct Interview Phase 2
Assess Interview Phase 2 outcome
Evaluation of the outcome
Assess the outcome
Finalize the proposed Processes for GDPR/PSD2 compliance
Final report

Figure 1 Formulation of Plan of Approach for research assessment

Firstly it is important to define the objectives of this study and translate them into the relevant research questions. This step will set the orientation of this study and the main ground in order to develop the next step which is the primary literature review. On this step we will get insight and understanding of the subject and will settle the foundation required to answer the questions set on the previous step. That consists of the documentation of personal data regulations as officially published by EU authorities. Next to the primary literature review, secondary sources such as articles and white papers will be reviewed in order to complement the knowledge of the main subject from market and business perspective.

The third phase consists of the preparation of the first interview round; not only is the list of the questions to be addressed required but also the need to specify the target group of the interviewees. In particular, their role/position, participation in relevant projects and their background, are considered key factors for the selection process. After, the interview phase one will take place by conducting the interviews online and recording the sessions. In the meantime, the questionnaires will be prepared and finalized on an online survey format, ready to be shared.

After questionnaire distribution, will move on with analysing the results both from the interviews and the survey. The outcome of this phase is crucial on formulating the interview round two, where the audience will be targeted based on their expertise, in order to be able to fulfil any gaps not covered/answered during the research phase 1 and that will support to answer the research questions.

Moving forward, the analysis of the second round of interviews is required to formulate our conclusions. Also, the outcome of this analysis will be the foundation for the process design of the steps that financial institutions must follow in order to be compliant to the regulations. Final step is to gather the outcome of the conclusion assessment, revise the conclusions and be able to formulate the final report. The expected outcome will be process flow approach which will be consisted of the mandatory requirements towards GDPR and PSD2 compliance, as regulatory obligations, as well as some best practices that the banking organizations have developed to support their existing processes around personal data.

3. Literature Review

This chapter captures the initiation of the research process which is the review of the existing literature that will support the development of our topic furtherly. Due to the nature of our topic, that the trigger is the publication of new regulations on personal data management, we mainly have to review the official published material by EU. In particular, we will focus on the main principles captured in the Articles of GDPR publication, as well as on the official guidelines on how FIs are imposed to implement personal data assessments. Therefore, we will be able to understand the importance of the new roles introduced, the customer consent mechanism and the data minimization concept and interpret those to requirements for banks to fulfil.

3.1 GDPR (General Data protection Regulation)

3.1.1 Introduction in GDPR

The importance of providing high quality of personal data, especially in the financial sector, has led the EU to introduce GDPR; GDPR is fully in force per May 25th, 2018 in all member countries of EU and aims to harmonize data privacy laws within Europe.

At this point it is important to give some important definitions of legal terms and that will often appear in our research thesis.

Personal data; as any information that is related to identify a living individual. Also, any other pieces of information, collected together, that can lead to the identification of a particular person, is also defined as personal data and falls within the scope of the GDPR. Personal data that have been shared and anonymized in a manner that the individual is not identifiable, is not considered personal data [2].

Some examples of personal data;

-name and surname

-address

-email address such as surname.name@company.com

-ID card number

-Internet protocol (IP) address

Examples of data not considered personal data:

-an internal company registration number

-email address such info@company.com

-anonymised data

Data processing is any action performed on data, automated or manual. Potential activities that are considered processing of data are collection, record, storage, deletion, structuring [4].

Data subject is the person whose data is processed; such as clients of a banking organization.

Data controller is the person or company who decides the purpose and the means of data processing. When it comes to privacy laws, the data controller is responsible to protect the privacy and the rights of the data subject [5].

Data processor is the person who processes the data that is given to him by the data controller. It is very common that a data processor can be a third party that is hired or imposed by the controller in order to process the personal data [4]. In any case, the owner of the data is the data controller and the means and purpose of data processing still lie under his authority

In the light of the definitions and the given examples, the regulation states that personal data should be protected regardless of the way of processing and storing it or even the technology used; it can be stored in a Database, on paper or through surveillance camera [2].

The official subject matter and objectives of GDPR are stated in Article 1 as per below:

1. GDPR lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
2. GDPR protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.
3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

The scope of the regulation is not limited only to EU borders, as it is also applicable when someone processes personal data or services of EU residents and citizens.

3.1.2 Principles

By the publication of six privacy principles it is easy to underline the core purpose and the essence of GDPR that differentiates it from previous personal data regulations [6].

1. Personal data should be processed in a Lawful, Fair and Transparent way, in respect to the individuals
2. Limitations on the purpose of collection, processing and storage of personal data. The data should be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. Data Minimization which means that the data should be adequate, relevant and limited to the purposes that they were stated for processing.
4. Accuracy of data so that it is up to date and necessary. Any data that is not accurate should be erased or rectified.
5. Data should be stored in a form that permits identification for no longer that is necessary for the purposes that have been agreed for data processing (how long the data can be processed/stored)
6. Integrity and Confidentiality; the data should be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

For each member state of the EU the concept of Data Protection Authority (DPA) has been introduced. The scope of our assessment is limited to financial services organizations in the Netherlands and therefore lies under the Autoriteit Persoonsgegevens (Dutch DPA). The main responsibilities of a DPA are to supervise whether the law is violated, consult with regards to the interpretation of the legislation and assess codes of conduct. In addition, the Dutch DPA is cooperating with the rest of DPAs among EU to ensure compliance to the laws and participates in the European Data Protection Board (EDPB) [10].

Consent

Another aspect that GDPR highlights is the consent; especially for the purposes defined for the data processing. At this point it is important to describe the consent in relation with the definitions given above. The data subject should give his consent, in an explicit way that he/she is aware of the purposes that the data are going to be processed for. Also there should be transparency on the legal basis of data processing as well as who is going to be the data processor, especially when the data controller is hiring third as data processor.

The means used to get the consent of the data subject should be clear and in an easily accessible and affirmative way, without leaving the field for misunderstandings or unclarity. For example it can be a form that needs to be signed or a tick in box.

At the same time, the data subject has the right to withdraw his/her consent any time [7].

Data protection by design and by default

The controller has always the responsibility to implement all the relevant measures, on organizational and technical level, in order to ensure that by default, only the personal data required for the purposes of processing stated, are to be processed (data protection by default) [8]. Data processing should be limited to achieve the relevant purposes set, ensuring processing only the data required and for the timelines agreed, while the individual has sufficient choices to exercise his/her rights [9].

In order to guarantee that, the nature, scope and risks of data processing need to be determined upfront, on the design phase, so that the risk of not complying to GDPR to be eliminated (data protection by design). In other words, data protection should be integrated in all the data processing activities, in terms of system, process and physical design, and needs to be guaranteed throughout its lifecycle while always protecting individual’s rights [8].

3.1.3 Data Protection Impact Assessment (DPIA)

A DPIA or also known as PIA (Protection Impact Assessment) is a concept tied to GDPR introduction (Article 35) and has so far been a systematic and very effective tool for the organizations to assess their privacy levels. This assessment can be done from multiple angles such as data, systems and processes. Most of the FinTechs tend to do this exercise on data level; by defining the flows of data among the multiple systems it is easier to identify risks and flaws, understand the purpose of data usage and ultimately be able to prove compliance to privacy obligations [17]. Apart from accountability, DPIAs are supporting controllers to prove that appropriate measures have been in place to guarantee compliance too [19].

As indicated in Article 35, a DPIA is required on cases described as below. The exact wording focuses on “likely to result in high risk” which is detailed on DPIA guidelines section:

-Personal data related to Natural Persons, when there is systematic evaluation as well as data processed in automated way such as profiling, and on which decisions are based that can cause legal effects or affect the natural person [19].

-Processing at large scale of special types of data like racial, ethnic, political opinions, genetic, biometric and health data [18], as well as data that can lead into decisions on legal effects on a natural person.

-Systematic monitoring of a publicly accessible area on a large scale of data.

In summary, DPIA is a process for building and proving compliance; aiming to spot risks related to the processing of personal data and eliminate them. This assessment cannot be limited to one-off logic; organizations should be able to perform it anytime and in cases the risk factors are changing.

DPIA Guidelines

The European Commission, next to Article 35, has published the guideline document named as "Guidelines on DPIA and determining whether the data processing is "likely to result in high risk" for the purposes of the Regulation 2016/679". The purpose of this document is to capture the scope of a DPIA and assess the need to capture and manage risks and rights of natural persons while processing personal data.

The obligation for controllers to conduct a DPIA in certain circumstances should be understood against the background of their general obligation to appropriately manage risks presented by the processing of personal data [19]. That makes DPIA a risk-oriented approach and it imposes a detailed risk management approach where all risks are identified, analysed, estimated, evaluated, mitigated and reviewed on a regular basis.

The decision tree below describes the basic principles and whether a DPIA is required.

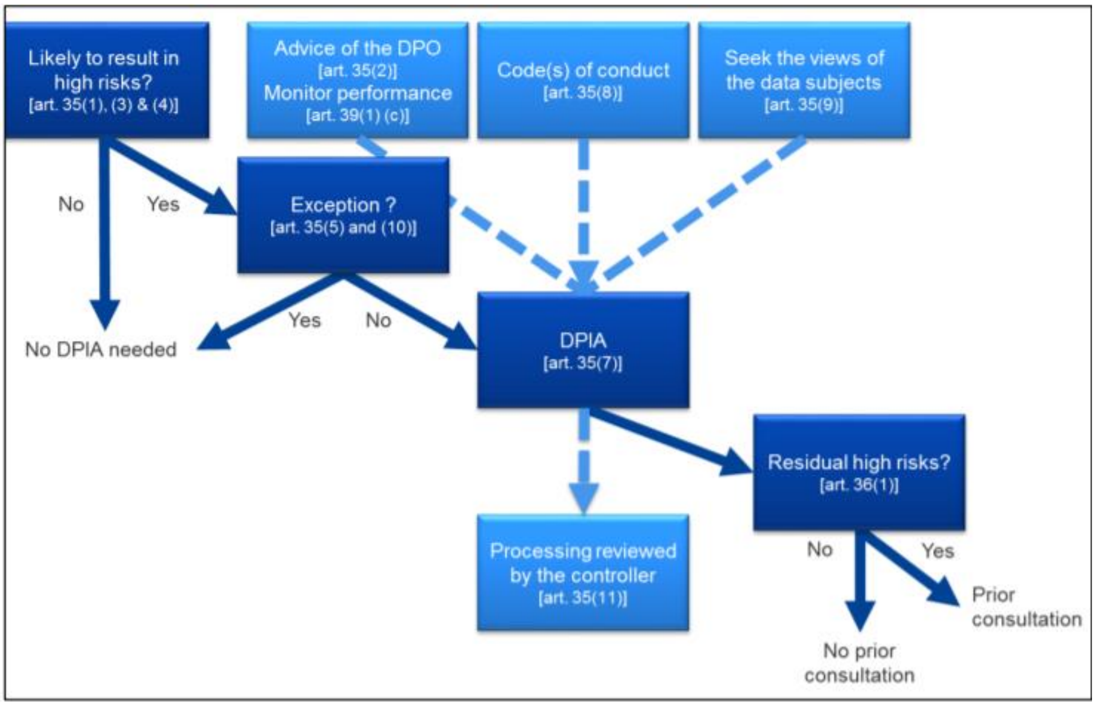

Likely to result in high risks? [art. 35(1), (3) & (4)]
Advice of the DPO [art. 35(2)] Monitor performance [art. 39(1) (c)]
Code(s) of conduct [art. 35(8)]
Seek the views of the data subjects [art. 35(9)]
No
Yes
Exception ? [art. 35(5) and (10)]
No DPIA needed
Yes
No
DPIA [art. 35(7)]
Residual high risks? [art. 36(1)]
Processing reviewed by the controller [art. 35(11)]
No
Yes
Prior consultation
No prior consultation

Figure 2: Basic Principle of DPIA in GDPR. Source [19] – page 7

A single DPIA can be used to assess multiple operations around data processing, as far as the purpose, scope, context and risks are similar. That simplifies the job of the controller and gives accessibility and portability options. In cases of joint controllers, the responsibilities should be defined precisely and therefore the obligations too [19]. The guidelines also describe how useful a DPIA can be for assessing the impact of a technology product. Although it’s always the controller's responsibility to conduct a DPIA, there can be situations where there is a suggested way to implement an assessment that can be adopted by different controllers for different processing operations [19].

Next to the elements of Article 35, the guideline documentation defines in detail nine criteria in order to set a more concrete instruction on the cases that require a DPIA.

1. Evaluation or scoring, including profiling, of aspects like economic situation, location, movements of the data subject; e.g. a financial institution that screens clients against a credit reference database for AML or fraud.
2. Automated decision making with legal effect; e.g. exclusion or discrimination of individuals while screening.
3. Systematic monitoring. This criterion for occasions where the data are collected through networks and therefore the data subject may not be aware who collected the data and how they will use it.
4. Sensitive or highly personal data such medical data, criminal records.
5. Data processed on large scale; although there is no specific definition on large scale, there are some factors to take into consideration such as the number of data subjects (population), the geographical scope of the assessment, the volume of data together with the duration that will be required for the assessment.
6. Match or combination of datasets, in cases where multiple assessments to be executed by different controllers and for different purposes.
7. Data concerning vulnerable data subjects; for situations where there is some sort of imbalance between the data controllers and the data subjects, with the last ones to require special protection (e.g. elderly people, mentally ill, asylum seekers).
8. New technological innovative solutions which may introduce new ways of collecting and assessing personal data, then DPIA is required in order to identify the risks and protect the data subject’s rights.
9. Prevention of data subjects from accessing a service, product or right, e.g.

DPIA flow, Roles and Responsibilities

A DPIA must be performed prior to the processing, so that it complies with privacy by design rules [17]; it’s a tool that would support the decision making around the data processing assignment. At this point it is important to highlight that DPIA is a continuous assessment, it should also be reviewed and re-assessed on a regular basis in order to guarantee compliance to portability.

It is always the data controller’s responsibility to conduct a DPIA; starting from the decision whether a DPIA is required and always in combination with the vision of data processing flow and potential measures. Next to that, the risk assessment would follow in relation with the rights of the data subject so as to provide a risk mitigation strategy. Finally, the controller should document and publish the DPIA but also be in charge of review and reassessment. The flow below [Figure 1] shows the standard steps required while executing a DPIA.

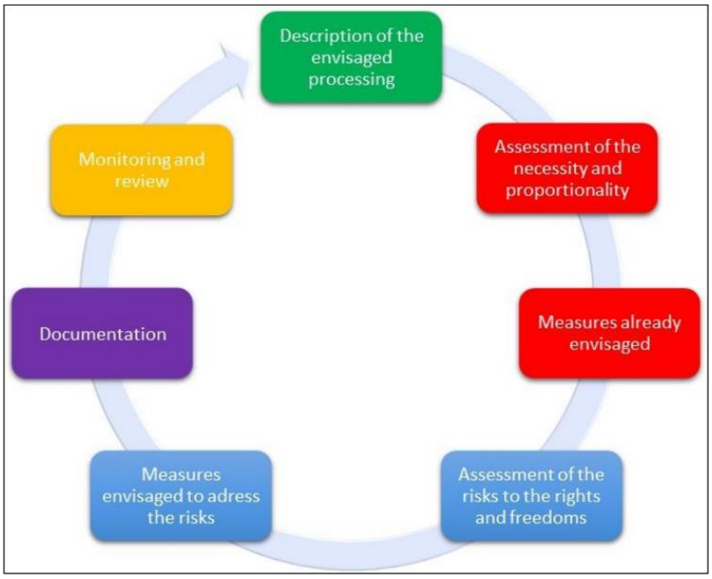

Description of the envisaged processing
Assessment of the necessity and proportionality
Measures already envisaged
Assessment of the risks to the rights and freedoms
Measures envisaged to adress the risks
Documentation
Monitoring and review

Figure 3 DPIA process flow, standard steps [19]

The importance of the role of the data controller has been emphasized multiple times; in particular while conducting a DPIA the RASCI table below summarizes the roles and responsibilities per step provided on Figure 1.

- The data controller is responsible for the whole life cycle of DPIA, although he can delegate it to a third party. The controller can also select the methodology that will be followed and also be able to seek advice not only to DPO and processor but also to other specialists such as IT, legal experts.
- The involvement of the data processor lies in supporting and providing input mainly on the design phase of the assessment where all the rights of the data subject should be specified as well as the purpose of data processing.
- The DPO needs to guarantee that the assessment is compliant to the GDPR principles for each and every step, but also able to consult the controller, even imposing a specific way of conducting a DPIA. In addition, it’s his/her responsibility to evaluate and review the relevant documentation.
- The data subject is not actively involved; however it is crucial that the risks and freedoms identified to be in line with the views of the data subject based on which he/she had given consent.

Activity	*Data controller*	*Data Processor*	*Data Protection Officer*	*Data Subject*
Description of the envisaged process	R	S	C	
Assess the necessity & proportionality	R	S	C	
Measures envisaged	R	S	C	
Risk assessment, rights and freedoms	R	S	A	I if applicable
Risk mitigation measures	R		C	
Documentation	R		A	

Publishing	R		A	I if applicable
Monitoring & Review	R		A	

Table 3: RASCI matrix for DPIA

The publishing step is not a legal requirement of GDPR, the decision lies on the controller whether it should be done. Nevertheless the DPIA guidelines provided, highlight that it should be taken into account publishing a conclusion or summary of the DPIA [19].

The activities defined above are quite crucial for the outcome of our research. Since we are aiming to a process approach with all the necessary obligations towards the regulator, these guidelines can set the orientation that the banking organizations should follow and set the path for transformation required not only on activity level but furtherly to the technology means.

3.2 Payment Services Directive 2 (PSD2)

3.2.1 Introduction and basic principles

Next to GDPR, since January 2018, the rules for payment services in the EU have been revised and they were published under the Directive (EU) 2015/2366 (known as PSD2). PSD2 gives the legal foundation for the further development of an integrated internal market for electronic payments within the EU [12]. In particular, it regulates the rights and obligations of the parties involved, such as consumers, companies, banks and payment institutions, as well as the conditions governing payment transactions and related information [13].

Aim and Key Points

The goal is to make international payments (within the EU) as easy, efficient and secure as the payments within a single country therefore it provides the necessary rules in order to achieve it. In the light of this goal, it seeks to open up payment markets to new entrants leading to healthy competition, wider choices and better prices for the consumers. It is important to highlight that this revision of the directive takes into consideration the growth and the innovation of electronic payments methods via internet or mobile applications, a fact that has changed the scenery of payment services in the last decade.

As payment services, there are defined the services enabling cash to be placed on or withdrawn from a payment account, as well as all the actions around an account operation such as transfers of funds, direct debits, credit transfers and card payments. The paper transactions are not in scope of PSD2.

The rules set out seem quite similar to the principles highlighted for GDPR, but of course they focus on the financial and transactional data in terms of [12]:

1. Security for online payments especially when it comes to safe authentication and minimization of fraud risk.
2. Transparency of conditions and information requirements for payment services.
3. Rights and obligations of users and providers of payment services.

At this point it is important to mention that, contrary to GDPR, PSD2 highlights the necessity of consent but the consent concept is not defined. Hence, that fact leaves some field for unclarity especially to parties who offer payment services and they need to adjust to both legislations. It will be part of our research to identify the differences on the definitions of the consent concept and how the organizations have reacted.

Goals of PSD2

By defining the goal of the payment regulations we get a deeper insight on the vision of the regulators on how to improve the payment service market landscape.

-Ensure payment security and increase transparency

-Encourage innovation and healthy competition, by also allowing new players in the market

-Make within EU a harmonized payment system market

Open up the EU market to services and providers

In practice, PSD2 encourages new methods for making online payments and retrieving required information from bank accounts. In particular, the companies are encouraged to provide payment services based on the access to data about the payment account:

- Account information service providers (AISPs) by collection and storage of information, where the user is able to have an overview of his/her financial situation, among more than one bank at any time. This can be really handy for budget planning and/or financial advisory [14].
- Payment initiation service providers (PISPs) where a provider of payment services can initiate a payment from an individual’s bank account. The provider sends a request to the bank on your behalf and then the bank proceeds with it [14].

By that new providers will be allowed to access the market and increase the competition. However, the client needs to give his consent on whether the provider can access bank account data and agree explicitly on the purpose of using it [14].

Comparing PSD2 to its predecessor PSD1 quite a breach is noticeable; the introduction of TPPs (Third Party Providers) as a definition to regulate the new types of payments as described above. [23]

From PSD1 to PSD2

At this point, it is important to briefly refer to the PSD1 principles. PSD1 (Payment Services Directive 1) was introduced in 2009 with the main target to harmonize the payment services among the EU but also enhance transparency and legit market competition.. Quite a significant progress has been noticed on technological innovation as the last decade was the era of the outburst of e-banking, mobile banking applications etc.

Although the main principles of PSD1 are also reflected in PSD2, there are some key differences. Firstly, PSD1 was applicable only to payments executed in the EU and therefore only in Euro or any other state member currencies. Under PSD2, the scope is not restricted to geographical borders as it is applicable to any payments that either the payer or the recipient is located in the EU. This change is impacting any PISP outside the EU [24].

The second important change is related to the supervision authority. Based on the PSD1 approach, the local Financial Conduct Authority is responsible for the supervision and authorisation of PISPs whereas under PSD2 the responsibilities lie on the DPAs of each country as well as their cooperation and coordination under the umbrella of European Data Protection Board [24].

Authorisation of payment institutions - Supervision

In order for the payment institutions to be able to accommodate the services described in the previous section, they need to have been granted the relevant authorisation or licence. One of the requirements is some sort of indemnity insurance as a condition of authorisation. Also, they are strongly related with aspects such as the financial soundness of those institutions as well as their conduct towards businesses and individuals and the protection of personal data [16].

For each EU member the local national authorities are responsible for supervising payment institutions. In principle, every payment institution’s supervision falls under the local authority of the country where the office is legally registered. Since the institutions can also operate in any other EU member state then they can also fall under foreign supervision. For those kinds of cases that fall under foreign supervision, the local relevant authorities have to collaborate if necessary when any issue occurs.

3.2.2 New Security Requirements

Customer Authentication

One major development of PDS2 is known as SCA – Stronger Customer Authentication, which introduced two new factors in the financial institution operations that were not required previously; with regards to payments and the access online to bank accounts as well as a strict definition of what can be considered an authentication factor. It is expected that we will move from the traditional authentication method, for example card number, expiration day and CVV, that are written on a card, to a more secure and sophisticated method [20]. The elements used for authentication should be now more advanced and will be using verifications most likely via SMS on mobile phones where a code will be valid only for a single transaction.

The SCA subject could raise security and privacy risks for the customer or/and the PISP. In order to simplify the SCA process and make it more understandable and feasible for the users, by requiring two out of the three below [24]:

1. Something the customer knows, such as a password or an answer to a question.

2. Something the customer has, such as a bank card or a mobile phone.

3. Something the customer is, such as biometric data (fingerprint, facescan)

The requirements of SCA apply to payments initiated by the payer, regardless of the fact that the payer can be a natural person or a legal entity.

Central Contact Points

In March 2019, there was a supplementing memorandum published by the European Commission with regards to the adoption of draft standards by the EBA in order to appoint the circumstances where a central contact point needs to be appointed as well as the functions of those contact points.

Therefore some criteria have been defined for payment institutions to appoint a central contact point when one or more of the followings is true [21]:

1. The total number of agents through which a payment institution provides any service under the right of establishment in the last financial year is equal or exceeds 10.
2. The total value of payment transactions in the host Member State, including transactions initiated and carried out by a payment institution, exceeds 3 million euros and the institution has engaged at least two of those agents under the right of establishment.
3. The total number of payment transactions carried out by a payment institution in the host Member State in the last financial year, including the number of transactions initiated, exceeds 100000 and the institution has engaged at least two of those agents under the right of establishment.

Next to the criteria described above, the obligations of those contact points have also been included in this memorandum. In particular each contact point [21]:

1. Shall serve as a single provider and single point of collection for reporting obligations of the appointing payment institution towards the authorities of the host Member State.
2. Shall serve as a single point of contact for the communications between the payment institution and the authorities of the host Member State.
3. Shall facilitate the on-site inspections by the authorities of the agents of the appointing payment institution in the host Member State.

IT solutions

It is very clear that the security among payment institutions systems needs to be increased in order to facilitate the new requirements that PSD2 brought. Although it has not been explicitly described in PSD2 documentation, in the financial sector most of the technology solutions are now oriented towards the Application Programme Interfaces (APIs). Those interfaces allow not only the share of data between AISPs and PISPs, but also can contribute to standardizing the communications across banks and service providers [15]. This digitisation initiative increases the IT costs but in the market there is a lot of movement of big banks that collaborate, also with FinTechs, in order to centralize innovation and provide customer focus solutions.

3.2.3 EBA Guidelines on ICT and security risk management

First publication June 2019

In November 2019, the EBA has published the final report with the ICT and security risk guidelines. The purpose of that publication was to describe and detail how the supervision should be done in terms of security and ICT risks [25] with ultimate goal to have a governance framework in place in order to mitigate those risks.

By ICT and Security Risk, Article 95 of PSD2, defines the operational risks of the payment services due to their electronic nature. This type of risk is precisely defined as such in order to avoid confusions and misunderstandings compared to other kinds of risk such as compliance, legal or reputational [25].

The scope of those guidelines is specified as such: it covers PSPs for their payment services (including issuing electronic money), credit institutions for their activities beyond their payment services and investment organizations for all activities [25]. They provide also specific guidance on the reporting requirements that FIs have to fulfill within the European System of Financial Supervision.

Strategy and Governance

In summary, the financial organizations need to ensure that [25]:

-the required controls and governance are in place

-their employees are sufficiently trained and qualified

-their business plan should include those activities and define clear accountability

The above need to be well described as part of the overall ICT strategy and it is necessary not only to monitor the relevant actions but also review those on a periodically basis.

When it comes to the TPPs, the EBA guidelines on the outsourcing arrangements (EBA/GL/2019/02) define the requirements to be met by both sides. There is highlighted the importance of the data agreements or the service level agreements to include the clear objectives and measures around specific elements such as network security, data encryption specifics, cybersecurity etc. As well as the necessity to have in place the relevant procedures for incident handling, escalation and reporting [25]. Particularly, the major operational or security incidents should be classified, on the format, the content and the procedures, including standard templates as well as the criteria are defined on how to assess the incidents [26]. Roles and responsibilities should be clearly defined together with the reporting line to be followed.

Next to the governance, it is required to document the information assets, the systems and processes that those assets are flowing, both internally and externally, and the parties involved, especially the third parties [25].

Revised Guidelines June 2021

The first ICT and security guidelines were initially published in 2018 and were applicable since early 2019. The banking organizations had reporting obligations towards the local supervisory authorities. After some months of following the proposed reporting procedures, it seemed that some steps were quite time consuming while not important enough to facilitate the ultimate reporting purposes [26]. The revised guidelines will be applicable by January 2022.

As a consequence, the authorities while receiving the reports, in combination with the complaints filed, they were urged to revise the guidelines. It was observed, that the way the PSD2 requirements were implemented, was not common across the different EU countries.

Summarizing the new guidelines, the two most important points for improvement to mention are:

1. The new guidelines were aiming to simplify the reporting procedure by eliminating unnecessary steps and providing standard templates. Also, the content of the report should focus on the major incidents that impact PSPs [26], therefore the quality of the report to be enhanced.

2. In regards to the classification criteria, next to some updates of the description of the existing ones, there was new criterion introduced is called " Breach of security of network or information system" (previously known as "Breach of security measures"). By bringing this change, the aim was to eliminate the scope of the criterion, which in the first place was considered too broad, and simplify the assessment and implementation requirements [26]. That was mainly driven by the feedback received from the public consultation.

DORA

In the meantime, EBA is already working on the next regulation, estimated to be published in 2024/2025. There are ongoing negotiations on the European Commission's proposal for an EU regulatory framework on digital operational resilience (DORA), which will be used to streamline and harmonize the ICT reporting, to all financial services provided by all FIs among banking, investment management and insurance [26]. It is estimated that as soon as DORA will be applicable the revised guidelines will be unnecessary.

3.3 GDPR and PSD2

Due to the timing of GDPR and PSD2 publications and also the possible relevance between the legal basis of the client consent, a lot of discussion has been raised in the financial world whether those two are truly related in a way that the main principles and implementations required can be combined or covered simultaneously. We ran into a lot of articles and papers aiming to compare the main principles of each regulation and how those can be translated to internal activities for the banks. The purpose of this chapter is to investigate and understand whether GDPR and PSD2 are related in a core sense and any potential approach that will facilitate compliance requirements for both.

3.3.1 Balance between GDPR and PSD2

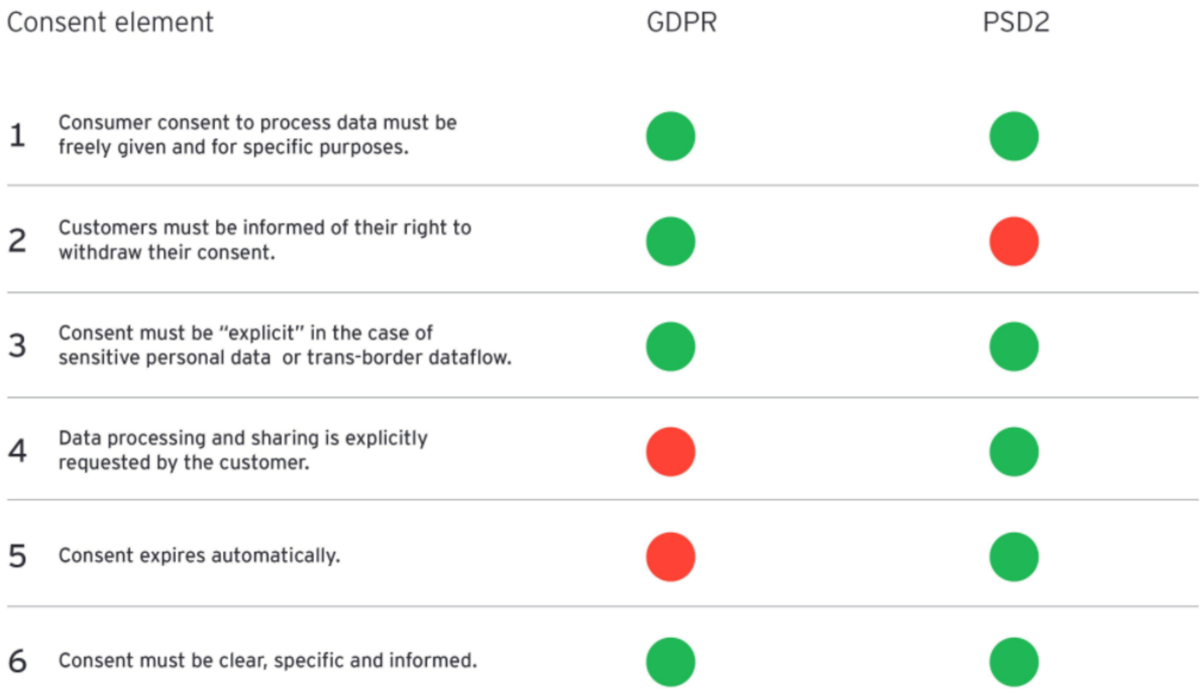
GDPR was introduced in order to assure protection of personal data while PSD2 aims to reshape the way banks and other institutions perform their transactions. Therefore the challenge of the Financial Services domain is heavily impacted by the introduction of the two regulations in such a short period of time.

At first glance, the regulations seem to have quite a few similarities but it is important to highlight that they were developed on different legal bases. GDPR focuses on the protection of personal data and raising awareness on the clients how, when and for which purposes their data are used. Meanwhile, PSD2 by providing authorisation to third parties of accessing account information through AISPs and PISPs described earlier [15].

Considering this overlap between the two regulations, the traditional financial institutions can allow TTPs to access personal data only by complying with GDPR; a fact that increases the complexity of the protection of data.

3.3.2 Client Consent Mechanism

The element that is considered the common ground between GDPR and PSD2 is the consent mechanism. In GDPR it is stated that data cannot be processed without the client consent whereas in PSD2 the consent concept is mentioned but not defined. The table below summarizes the differences between the two legislations.



	Consent element	GDPR	PSD2
1	Consumer consent to process data must be freely given and for specific purposes.	🟢	🟢
2	Customers must be informed of their right to withdraw their consent.	🟢	🔴
3	Consent must be "explicit" in the case of sensitive personal data or trans-border dataflow.	🟢	🟢
4	Data processing and sharing is explicitly requested by the customer.	🔴	🟢
5	Consent expires automatically.	🔴	🟢
6	Consent must be clear, specific and informed.	🟢	🟢

Table 4 Differences between PSD2 & GDPR in regards to the Client Consent Concept. Source EY whitepaper [15].

PSD2 states that “payment service providers shall only access, process and retain personal data necessary for the provision of their payment services, with the explicit consent of the payment service user”. In the meantime, the European Data Protection Board (EDPB) has clarified that the “explicit consent” referred to in PSD2 is a contractual consent, as payment services are always provided on a contractual basis between the payment services user and the payment services provider. Therefore, as set out below, the concept of payment service user “consent” for purposes of PSD2 should not be confused with the concept of data subject “consent” under the GDPR. [22] It appears that the consent for PSD2 is one-sided and should be established between the customer and TTPs. However, most of the banks have received complaints on that matter, since it was not clear that the consent should be given directly to the TTPs rather than the bank.

3.3.3 Conclusion GDPR-PSD2 relation

Although in a first impression it seems that there must a be a correlation between the two regulations, by diving on a detailed level there are some key differences that they do not allow misconceptions especially on the consent mechanism. The main outcome of the comparison can be that in an ideal environment that banks are sufficiently compliant to both regulations, they can be considered complimentary and able to enhance the personal data privacy of customer and transaction data, like an holistic approach for optimization of data management processes.

3.4 Literature Review Conclusion

The purpose of conducting the literature review was to get a deep understanding of the regulations and get acquainted with the guidelines provided in order to achieve compliance. Yet the available material was not sufficient enough in order to answer the research questions. By diving into each regulation there were certain topics that caught more attention but also there were defined quite challengeable during the implementation processes.

The table below summarizes the topics identified per regulation that we will focus in the next phases of our research.

Regulation	Topic	Challenges
GDPR/PSD2	Impact of the new publication	How the banks will reach upon it
GDPR	Roles introduced	If the roles are applicable How there were introduced Contribution to supervisory obligations
GDPR	Personal Data Assessments	How there were introduced On which level there are performed
GDPR/PSD2	Client Consent	Impact on the relationship with the clients
GDPR/PSD2	Trainings	Importance, Preparation and Execution
GDPR	Data minimization & sanitization	What methods can be used, on which systems Impact on existing IT infrastructure
PSD2	API solution	Implementation Open up to the TTPs
PSD2	ICT and security requirements	Reporting incidents Revised Guidelines and impact

Table 5: Literature review conclusions’ overview.

4. Research Conduct

Following the literature review and the outcome of it, it was necessary to define the next steps of the outreach to the specialists and set a strategy in regards to the interview plan and the questionnaire. The process of planning the interviews required some preparation steps in order to arrange the sessions with the interviewees. In particular, the steps followed were:

-Search among business network and create a pool of interview candidates, involved in GDPR and PSD2 activities or projects.

-Select the most relevant candidates based on their involvement in GDPR/PSD2 activities, considering their role, seniority and expertise.

-Approach the candidates, expressing interest for interview and setting the context, objectives and purpose of the interview session.

-Arrange the interviews, on agreed time and date and share the main points for discussion.

-After the interview, ask for relevant contacts that could contribute to the research but also leave the field for questions and feedback.

4.1 First phase of interviews

4.1.1 Design of interview phase & objective

In the first research phase our aim is to have three semi-structured interviews with experts/specialists that work currently (or have worked) in the implementation of GDPR and PSD2 projects.

The purpose of this round is to explore the initial reactions in regards to the publications of personal data regulations back in 2018-2019, in particular considering the aspects below:

a. Impact, compared to the previous regulations.
b. The new roles imposed and the manner there were implemented.
c. The new assessments and how they were executed and implemented.

The questions addressed were accordingly adjusted per interviewee and can be found later at the appendix. However, the discussions were structured based on the following sequence:

-Introduction – share of experience and background information.

-Goal of the interview sessions.

-Role and responsibilities of the interviewee in the GDPR/PSD2 related activities.

-New requirements/actions imposed by the new regulations, in terms of roles, responsibilities, assessments.

-Challenges along the implementation.

The selection of roles was carefully decided after finishing the literature review; the intention was to include people involved from the legal side as well as from implementation perspective. The table below summarizes the main information about the three interviewees.

Interviewee Code	Role	Seniority	Landscape	Financial Services Domain	Regulation Focus
A	Project Manager	Senior	Consultancy Services	Cross-domain	GDPR
B	Data Privacy Officer	Senior	Compliance	Banking Organization/ Bank A	GDPR/PSD2
C	Program Manager PSD2	Senior	IT	Banking Organization	PSD2

Table 6 Interview Round One – Participants' Overview

At this point it is important to mention that for this exploratory round the aim was to find a balance among the interviewees and their focus on the specific regulations.

Interviewee A has been involved in GDPR related projects, while Interviewee C on PSD2. Interviewee B contributed on questions related both to GDPR and in lesser extent to PSD2.

4.1.2 Interview Conduct & Outcome

Due to Covid-19 pandemic situation, it was not possible to conduct the three interviews in person, therefore there were scheduled, conducted and recorded online via Microsoft Teams and Google Meet. The transcriptions can be found in the Appendix under section Interviews' Transcriptions < First Phase.

The outcome of those interviews was used for the second phase of the research and as a baseline in order to formulate the Online Survey.

The main outcomes for this round of interviews are defined as per below:

GDPR

The questions were initially focused on how the impact of GDPR was considered in regards to the previous regulations. From legal perspective, GDPR was more like a formality that EU has imposed. The essence of the law was not that far from the predecessor, but the attention it caught on society and the need for social awareness, made the financial organizations to invest a lot on the implementation of GDPR. Starting with the review of the regulation by legal and compliance experts, the organizations had to specify the requirements and translate them to IT requirements. At early stage, the relevant projects have been formulated and formalized within the banks, gathering specialists from multiple angles of the bank.

As described in section 3.1.1, there are specific roles around data processing that each organization has to introduce. During this phase of interviews, there were questions explicitly referring to the definitions of the roles, focusing on whether there was awareness about those roles as well as if and how there have been introduced in the banks. Interviewee A as a consultant, explained how they have to focus on the data process itself in order to specify the responsibilities of the data controller vs the ones of the data processor. In the meantime Interviewee B as DPO could clearly state that in Bank A, the system owners were appointed as data controllers. Also the DPO and chief DPO roles were appointed on local and global level, considering the structure of the organization. In regards to third parties that act as data controllers, the relevant data agreements must be in place.

Next to the roles, there were also introduced the assessments of personal data, as mentioned in section 3.1.3. The banks were obliged to perform the DPIAs in order to create an inventory of the systems that manage personal data and the risks around the data processing. Each bank could select on which level they could perform the DPIAs and the most common way described on this round of interviews was to conduct a DPIA initially on system level. If necessary and considering the risks some banks could move further on asset level. Diving into more details with Interviewee B, in Bank A there are performing also some assessments before DPIAs, such as AIC (Availability Integrity Confidentiality) and based on the outcome of those they decide whether a DPIA is furtherly required.

PSD2

Following the same approach, for PSD2 the questions aimed to evaluate the impact of new publication, with main conclusion that it was not that major, compared to previous regulation. It was highlighted by the interviewee that the consent matter brought some confusion, as it was like an extra layer of consenting to the existing relationship with customers.

In terms of trainings, there were provided only to employees involved directly in PSD2 activities. In addition, some assessments were also introduced and extra controls were examined in order for the organizations to guarantee that they are PSD2 proof.

Comparing PSD2 and GPDR, the main difference was spotted on the detailed guidelines provided for GDPR, and not in PSD2. But also the necessity to have signed consent given mainly through the DDAs or DPAs, requirement that is not needed in PSD2. What was enhanced with PSD2, was the agreements with the third parties directly.

Finally, the need of reviewing the current situation and monitor it is covered by the Risk and Control Framework which, next to other risks, covers also the PSD2 related ones.

The table below summarizes the main topics covered in the first interview phase and the relevant outcome. This table was used as a baseline for the next phase of the survey. By applicable it means that the subject has been included in the discussion. By N/A as mentioned above it means that the subject was not covered during the discussion.

GDPR subject	Main interview outcome		
	Interviewee A	Interviewee B	Interview C
Comparison to predecessor regulation	N/A	Applicable Medium impact	N/A
Project based approach	Applicable	Applicable	N/A
Internal roles clearly defined and assigned	Applicable	Applicable	N/A
Client consent	N/A	Applicable Required	N/A
Data Agreements with third parties	Applicable	Applicable	N/A
DPIAs on system level	Applicable	Applicable	N/A
Review of DPIAs	N/A	Applicable Once in 2-3 years	N/A
PSD2 subject			
Comparison to predecessor regulation	N/A	N/A	Applicable Medium impact
Project based approach	N/A	N/A	Applicable
Trainings	N/A	N/A	Applicable

Extra assessments and controls	N/A	N/A	Applicable
Client Consent	N/A	Applicable Between client and third parties	Applicable Between client and third parties
Data agreements with third parties	N/A	Not necessary	Not necessary
Review process	N/A	N/A	Applicable Risk & Control Framework on yearly basis

Table 7 Interview round one – outcome & conclusions table

4.2 Survey Questionnaire

Following the plan defined in previous chapter, after finalizing the analysis of the first exploratory round of interviews, the key outcome topics to be covered have been identified. By using those as a baseline, the planning of the online survey conduct had to be defined.

4.2.1 Preparation Phase

The preparation phase of the Survey Questionnaire was divided in the following steps:

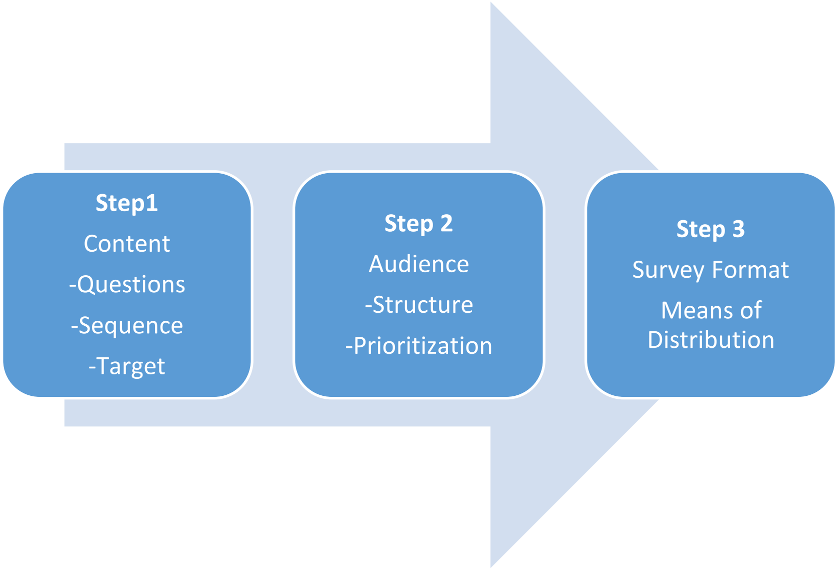


Figure 4: Online Survey Preparation Phase Plan

Step 1

The empirical method of questionnaire is quite essential in order to gain a better understanding on how financial services organisations reacted to the new personal data regulations. The aim was to have the questionnaire distributed to professionals from different departments and different backgrounds within banks, who can anonymously fill-in the questions. The questionnaire method allows us also to collect data from a bigger number of participants which would be quite difficult to achieve by interviews only.

Considering the outcome of the literature review and the first round of interviews, the questions were formulated as per below. The structure and the sequence was the same one followed during the interviews; the starting point was the personal experience and expertise questions, following on preparation and trainings as well as impact on IT requirements, implementations and challenges.

The survey was also split into two sections, each dedicated to each regulation and was presented as such:

Title: Survey about personal data regulations in Financial Service Organizations in the Netherlands.

Introduction:

1. For which sector of financial services are you working?
    a. Wholesale Banking
    b. Retail Banking
    c. Asset Management
    d. Other
2. For what department are you working?
    a. Legal/Compliance
    b. Data Management/Data Control
    c. IT
    d. Other
3. During your working daily routine, you deal with personal data on:
    a. Every day – Business as usual
    b. High-level involvement – project based
    c. Ad-hoc basis
    d. Never

GDPR awareness

4. How would you evaluate the changes that GDPR brought compared to its predecessor regulation?
    a. Major
    b. Minor
    c. No change
5. Did you follow any related course/seminar before the GDPR regulation went live in May 2018?
    a. Yes, internally provided
    b. Yes, by an external provider.
    c. No
6. Has your organization provided an internal training in regards to the implementation of GDPR?
    a. Yes
    b. No
7. GDPR describes quite explicitly the roles related to the processing of personal data; those are data controller and data processor. Are you aware of those roles among your organization?
    a. Yes, for both roles
    b. Only for data processor
    c. Only for data controller
    d. Not aware of those roles
8. Who acts as a data controller within your organization?

   a. Data management/control department
   b. Data Privacy Office
   c. System owners/ IT
   d. Higher management

9. Are you involved in activities related to the silent consent mechanism?
   a. Yes
   b. No
10. Do you agree with the legal basis of the silent consent concept?
   a. Yes
   b. No

   10a. Can you please explain your answer

11. In Article 35 of GDPR there are detailed DPIAs (data protection impact assessment). Within your organization on which level do you conduct those assessments?
   a. Data
   b. System
   c. Process
   d. Other
12. After the implementation for GDPR, have you been involved or have observed any exercise to make an existing system "GDPR proof"?
   a. Yes
   b. No

   12a. Can you shortly explain what kind of system that was and the purpose of data processing there?

13. After the implementation for GDPR, have you been involved or have observed any new system implementation?
   a. Yes
   b. No

   13a. If your answer on Question 13 was yes, can you please shortly state what kind of system and the purpose of processing data there.

14. From 1 to 5, how would you evaluate the implementation of GDPR solutions towards BAU?
   a. 1 very easy
   b. 2 relatively easy
   c. 3 neutral
   d. 4 quite difficult
   e. 5 extremely difficult
15. What was the biggest challenge while implementing GDPR related solutions among your organization? (More than one answers can be selected)
   a. The complexity of the regulation itself
   b. The complexity of the data landscape (data, systems, processes)
   c. The lack of relevant knowledge, sufficient trainings etc
   d. The lack of structure and guidance from higher management
16. What would you consider the key factors of success in implementing GDPR solutions? (More than one answers can be selected)
   a. Legal/Compliance bases

b. IT solution dynamics
c. Guidance from higher management
d. Culture among the organization

17. At this moment, three years after GDPR going live, how would you evaluate the current maturity levels of data privacy solutions in your organization?
    a. Initial
    b. Managed
    c. Defined
    d. Quantitatively Managed
    e. Optimized

PSD2 awareness

18. How would you evaluate the changes that PSD2 brought, compared to its predecessor regulation PSD1?

    a. Minor
    b. Major
    c. Neutral, not much change

19. Did you follow any related course/seminar before the PSD2 regulation went live?

    a. Yes, by an external provider.
    b. Yes, internally provided.
    c. No

20. Have your organization provided an internal training with regards to the implementation of PSD2?
    a. Yes
    b. No

21. Do you, in your daily work routine deal with transaction related personal data?

a. Yes

b. No

22. After the introduction of PSD2, have you participated or been aware of any new system implementation?
    a. Yes
    b. No

22a. If your answer on Question 22 was yes, can you please shortly state what kind of system and the purpose of processing data there.

23. Under PSD2, customer consent is cited as a necessary condition for the initiation of a payment order or the execution of a transaction. Are you involved in activities related to this mechanism?
    a. Yes
    b. No

24. Do you agree with the legal basis of the client consent mechanism?
    a. Yes

b. No

24a. If your answer on question 24 is no, please shortly explain why.

25. Do you agree with the following statement: GDPR and PSD2 share the same legal basis for customer consent?

a. Yes
b. No

25a. Please, explain your choice for question 25.

26. One major development of PDS2 is SCA – Stronger Customer Authentication, have you participated or observed any activities related to SCA within your organization?

c. Yes
d. No

26a. If your answer on question 26 is yes, please explain shortly the type of activities you participated/observed.

Step 2

Considering what would be the best approach to take the maximum advantage through this questionnaire, it was key to set the relevant audience. Because of the complexity of regulations like GDPR and PSD2, many professionals were required in order to cover all the dimensions such as legal, compliance, IT, data etc. Therefore, the target audience was defined as per below, per regulation:

Data Privacy/Protection or Compliance Officer (1 or 2)

Legal Counsel (3)

Data Controllers/ Data Stewards (1 or 2)

Consultants or PM on similar projects (4)

At this point, it is important to mention that the audience for PSD2 was more restricted, less number of participants found than expected based on the initial estimation.

Step 3

The questionnaire was transferred to an online survey tool, called "Google Forms" and it was distributed to 25 people via personal work network, university network and LinkedIn. The period that the survey was active was from late August 2021 until the end of September 2021.

The link shared can be found here:
https://docs.google.com/forms/d/e/1FAIpQLScU5j2hwhxfalDoqBzLv0TEmCRGh7ejfAJFerh-eSijxQRP0w/viewform

This survey is confidential and its findings are only served for academic purposes and scientific research.

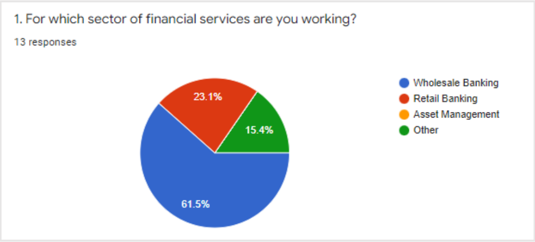
4.2.2 Questionnaire Survey Outcome

The online survey was available approximately for 40 days in Google Forms, on the 30th of September 2021 it was deactivated. Therefore, the next steps were to collect the questionnaire results and proceed with the analysis.

4.2.2.1 Survey Findings - General

The number of the survey participants was limited to 13 people, compared to the target of 25.

To start with, we defined the professional characteristics of the sample and their participation in every day work activities with personal data as per below:



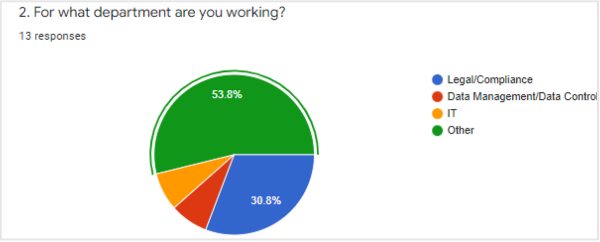


Figure 5: Participants position/expertise

Figure 6: Participants Department

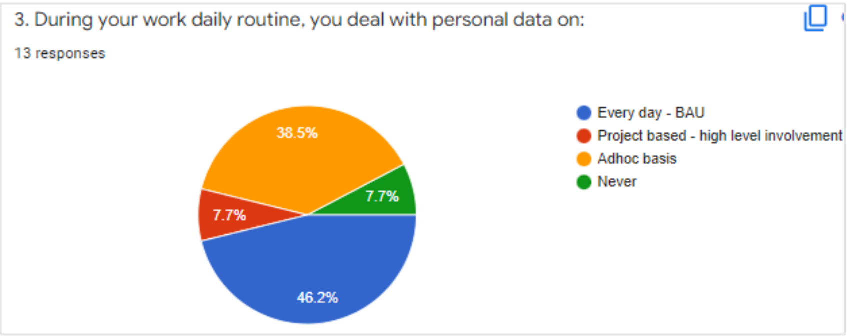


Figure 7: Participants' involvement with personal data

The majority of the participants work in the Wholesale banking (61.5%) but we see also 23.1% from the Retail sector. Important point to mention is that initially we were aiming to get an insight also in Asset Management organizations, in regards to personal data regulations. However, this goal has not been achieved since in the targeted network there were no responses from this kind of Financial Organizations. As a result our focus was restricted to Banks only, always with contribution from Consultants and Advisors from external firms, their characteristics for the questions above were included in the "Other" percentages. When it comes to the personal data related activities, almost 85% of the sample is dealing with it on BAU or on Ad-hoc basis, fact that proves GDPR and PSD2 could impact directly their work.

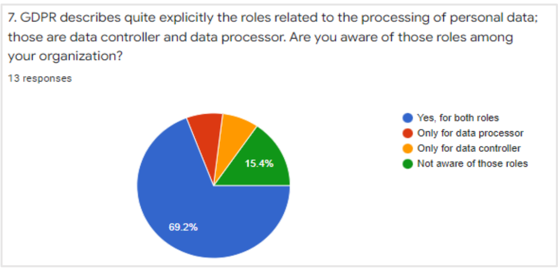
The conclusions from the finding section 4.2.2.1 were considered and included in the analysis for both the regulations of our scope.

4.2.2.2 Survey Findings - GDPR

Continuing with the questions' sequence, the next three ones were related to the impact of the new regulation and how there were prepared/trained before and after the implementation, In particular, the vast majority 84.6% evaluated the impact of GDPR publication in 2018 as major. Considering the awareness on GDPR importance, only 38.5% have been provided relevant trainings before GDPR going live. However we see that after the live date, approximately the 93% of the participants have been provided trainings.

After, the focus was switched on the roles that GDPR described and imposed to the organizations that manage personal data. As shown below 69.2% is aware of both the data processor and controller roles, while the 30% is ignorant about at least one of those roles.

Similarly, in regards to the data controller role and who is acting as such in banking organizations the answers given vary; the numbers are quite balanced between the DPO and the Data Management/Control department. But also the ones showing that higher management is acting as controller, seem quite interesting especially in combination with the previous question.



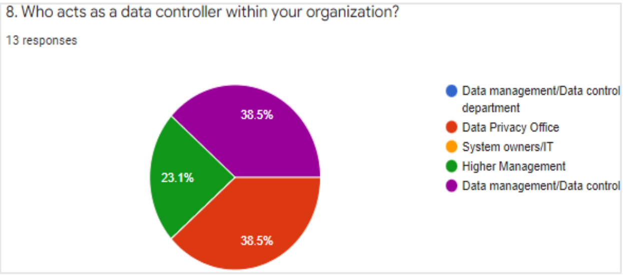
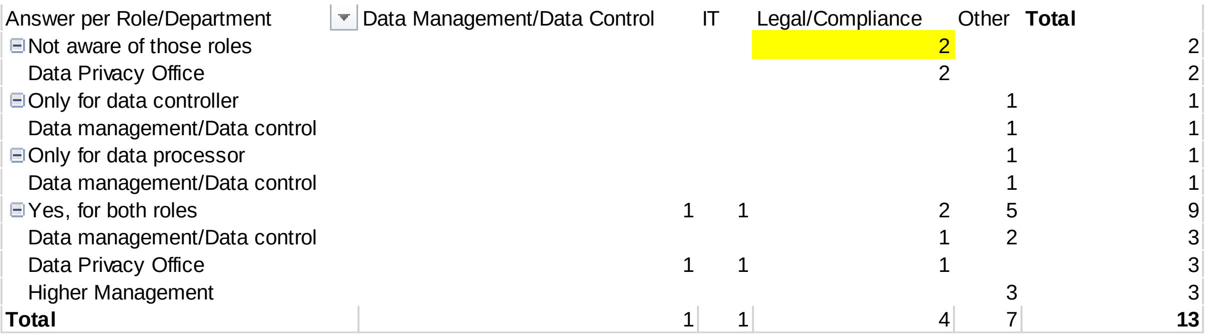


Figure 8: Data controller & processor role

Figure 9: Act as data controller

Considering the importance of the roles and the results of the last two questions, we dived into a deeper layer to verify from which parts of the organizations those figures derived. It seems that half of the participants from Legal/Compliance are not aware if the roles are implemented in their organizations. Similarly it is indicated for some external staff. Quite interesting finding considering that there was a three year period since the implementation and the training sessions provided in this timespan. But also how the respondents reacted on the controller role question and if there was a pattern identified.

The table below summarizes the results of Questions 7 and 8 based on the specialty of the respondent; the answers of who is acting as Data Controller really vary and no specific pattern was spotted.

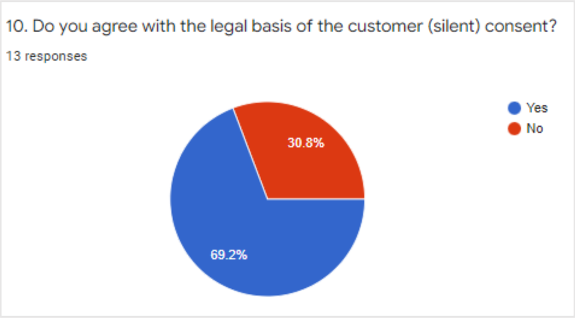


Answer per Role/Department	Data Management/Data Control	IT	Legal/Compliance	Other	Total
⊟ Not aware of those roles			2		2
Data Privacy Office			2		2
⊟ Only for data controller				1	1
Data management/Data control				1	1
⊟ Only for data processor				1	1
Data management/Data control				1	1
⊟ Yes, for both roles	1	1	2	5	9
Data management/Data control			1	2	3
Data Privacy Office	1	1	1		3
Higher Management				3	3
Total	1	1	4	7	**13**

Table 8 Data Controller Role among Banking Organization

One of the most important subjects of GDPR was the client consent mechanism and how it can impact the trust of customers. When it comes to the legal basis of it, we see that almost 30% disagree with the legal basis but the vast majority agrees with it and highlights by extra comment the importance of explicit consent required, next to the timeliness, purpose and manner of data processing.

Accordingly, the subject of DPIAs and on which level those are performed within the banking organizations was addressed through question 11.



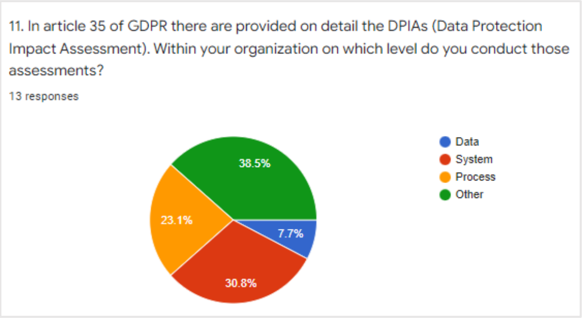


Figure 10 Customer (silent) consent – legal basis

Figure 11 DPIAs – level of performance

It is also interesting that 61.5% of the participants were aware of projects or IT implementations in existing systems that were managing personal data; where there are is a variety of activities that they contributed, such as processing personal data in payment systems, arranging data retention priorities in Data Warehouse as well as data storage localized. In regards to implementation of new systems, only one respondent mentioned the migration to new cloud provider in order to reassure personal data protection.

The timing that the survey was conducted, we could certainly say that GDPR related activities and processes have been already integrated to the daily work routine of bank employees. For the transition, from project phase to BAU, the statistics did not give a clear view; from 1-5, the values selected were between 2-4, avoiding the extreme easy and difficult.

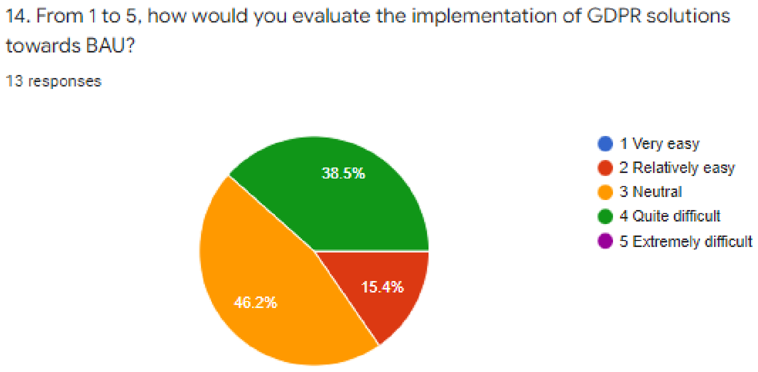


Figure 12 Project towards BAU - GDPR

The next two questions were focusing on the challenges along the implementation of GDPR but also which factors could be considered most key for a smoother transition. For those two topics, it is interesting to dive into a deeper level and check how the participants replied based on their positions/expertise. In particular, the complexity of the regulation itself is considered as a challenge not only from IT or Data Management specialists but also from legal or compliance ones. Similarly, the factors considered important to success we see clearly that from all different roles among the organizations, there is an almost balanced view, with leading one the Culture Factor, followed by the legal basis of the regulations and the IT implementation dynamics. The guidance of higher management did not seem to be a burden.

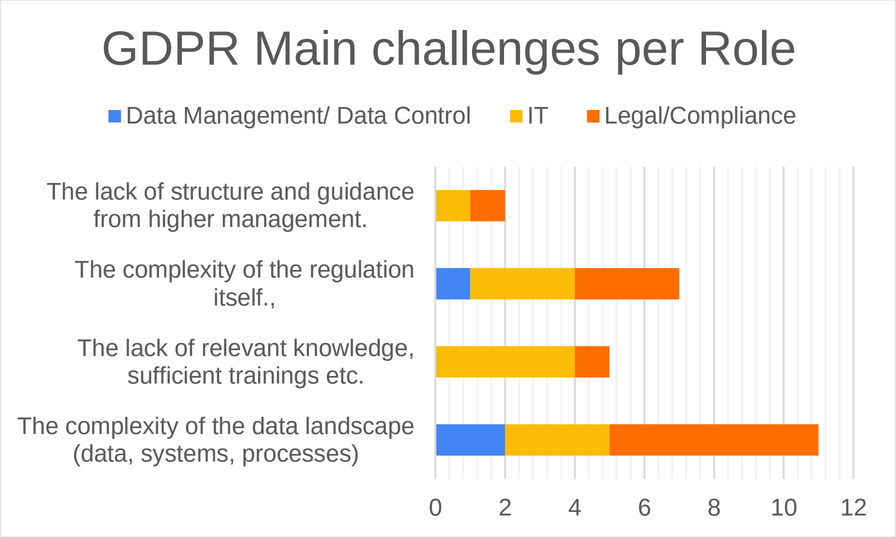


Table 9 Main GDPR challenges per Role

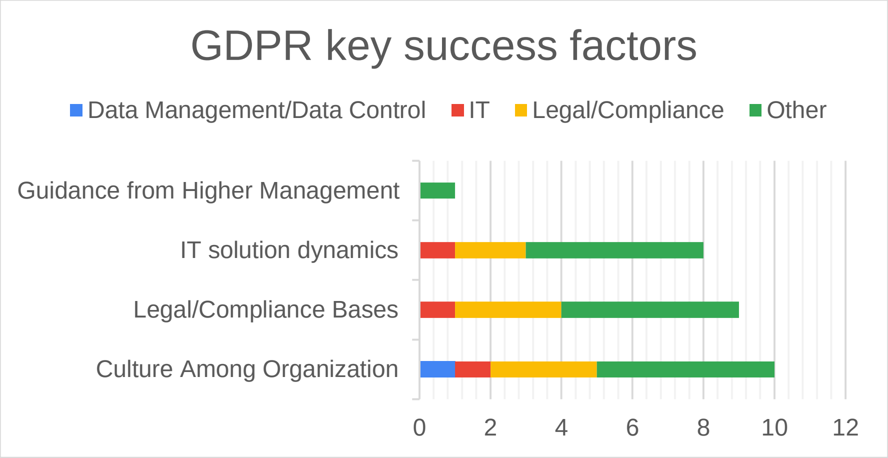


Table 10 GDPR key success factors per Role

To finish with the GDPR part, the last question was related to the current situation that the organizations stand and how mature they stand 3.5 years after GDPR went live. The vast majority of the participants is evaluating their banks on levels 3 and 4, which means that comply with the regulation but also the internal processes and controls are in place and documented. Also on level 4, the outcome of previous levels can be monitored and predicted, also to be used for future improvements.

The trends are also showing that legal and compliance employees tend to score the 4th level while for Other, there is no clearly statement, assuming the fact that they are dealing with more than one organizations.

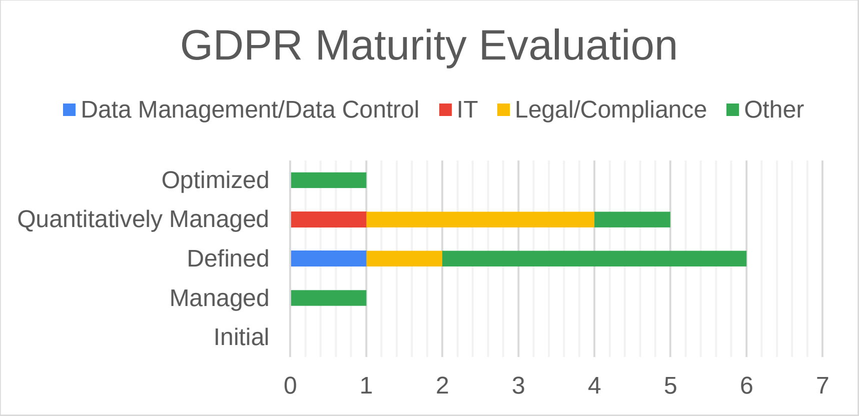
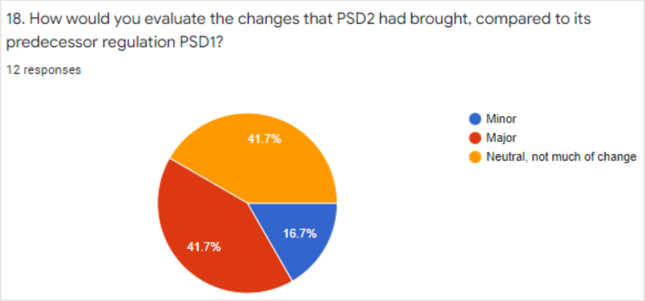


Table 11 GDPR Maturity Evaluation

4.2.2.3 Survey Findings – PSD2

Continuing with Section 2 of the questionnaire where the PSD2 related questions can be found.

Following similar sequence as for GDPR, we start with the impact evaluation of PSD2 compared to PSD1; equal number of participants found it either Neutral or Major, which seems quite contradictory. By diving into the role level, no specific pattern has been identified between the role of the respondent and the change evaluation. Again, it seems that Other category is also impacting the results in a more neutral way.



18. How would you evaluate the changes that PSD2 had brought, compared to its predecessor regulation PSD1?

12 responses

Table 12 PSD2 Impact

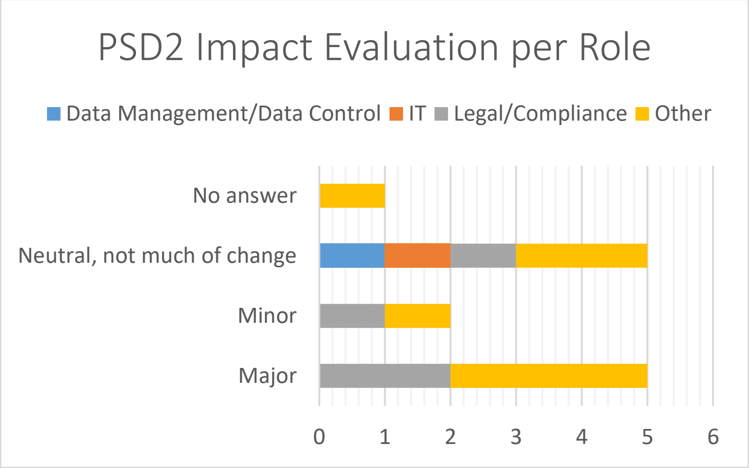
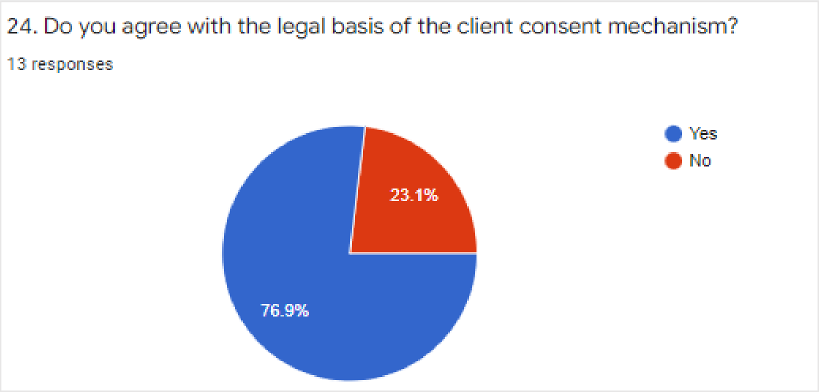


Figure 13: PSD2 Impact Evaluation per role

In regards to the trainings, it seems that limited number of people was trained before the PSD2 implementation but also after 23.1%. Only personnel closely working to the transaction processing was supposed to be trained. It was clear from the guidelines published by EBA that the banks had to open up their payment related data via APIs in order for TTPs to access it. Therefore, when in our questions system implementation is mentioned, it refers to the exercise related to the APIs and how they had to adjust them for opening up. Also one of the participants mentioned his/her involvement in a project of a subsidiary of big Dutch bank for the implementation of a payment system.

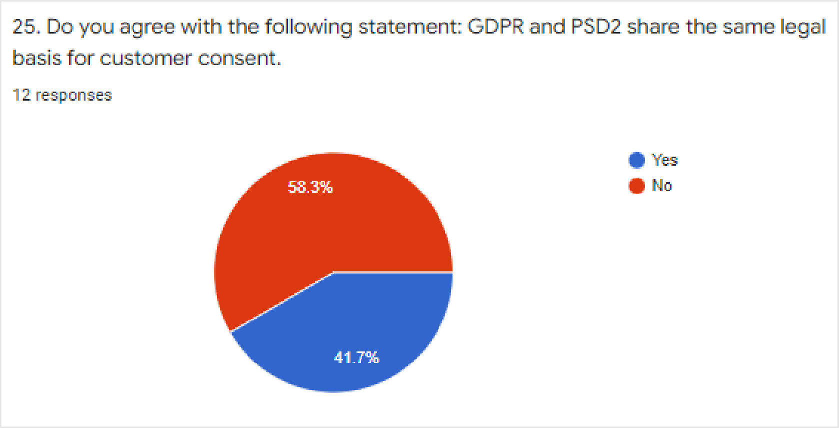
To continue with the consent topic, it seems that the vast majority 76.9% of our respondents agree with the legal basis of this mechanism, although it works differently compared to GDPR due to the involvement of TTPs.


24. Do you agree with the legal basis of the client consent mechanism?

13 responses

Figure 14 PSD2 – Client Consent Legal Basis

Additionally, the customer consent topic has raised a lot of discussion in the market on whether it is the meeting point between the two regulations, we have addressed that also in our literature review section. The 58.3% of the survey participants do not agree that the legal basis is common. By explaining their choice the most common comments were that PSD2 consent is one sided, as data processing can be initiated without the customer consent


25. Do you agree with the following statement: GDPR and PSD2 share the same legal basis for customer consent.

12 responses

Figure 15 Common legal basis of customer consent

Last question for PSD2 was related to the SCA and whether the participants have been involved in relevant activities. However, the responses were limited to two people, one of those has participated in project related to make stronger authentication for payments through mobile applications.

4.2.2.3 Summary of Survey Outcome

In order to compile the outcome of the survey, the same table formulated during the first phase of the interviews is used. The table is now enriched with the outcome of the survey; in particular because the number of participants was quite big to analyze the results per person, the findings were grouped per role. The percentages included are calculated as such: how many of the participants per role, have covered the subject. For example, for “Comparison to predecessor regulation” Out of total of 4 legal representatives, all of them answered that the impact was major. Therefore 100% Applicable.

Also, the subject list has been enriched with the additional topics that were covered by the questions. By Applicable it means that the subject has been covered in the answers of the questionnaire and by N/A that it was not.

GDPR subject	Survey Outcome			
	Legal/Compliance 4p.	IT 1p.	Data Management/ Data Control 1p.	Other 7p.Consultants incl.
Comparison to predecessor regulation	Applicable Major Impact 100%	Applicable Major impact 100%	Applicable Major Impact 100%	Applicable Major Impact 71.4%
Project based approach	N/A	N/A	N/A	N/A
Training afore	Applicable 50%	Applicable 100%	Applicable 100%	N/A
Training after	Applicable 100%	Applicable 100%	Applicable 100%	Applicable 71.4%
Internal roles clearly defined and assigned	Applicable 50%	Applicable 100%	Applicable 100%	Applicable 71.4%
Client consent	Applicable 75%	N/A	Applicable 100%	Applicable 71.4%
Data Agreements with third parties	N/A	N/A	N/A	N/A
DPIAs on system level	Applicable 25%	Applicable 100%	Applicable 100%	Applicable 28.5%
DPIAs on process level	Applicable 75%	N/A	N/A	N/A
Review of DPIAs	N/A	N/A	N/A	N/A
System Implementation	Applicable 75%	Applicable 100%	Applicable 100%	Applicable 37.5%
Maturity in control, adequate*	Applicable 25%	N/A	Applicable 100%	Applicable 71.4%
Maturity Optimized**	Applicable 75%	Applicable 100%	N/A	Applicable 28.5%
PSD2 subject				
Comparison to PSD1	Applicable Major 50%	Applicable Neutral 100%	Applicable Neutral 100%	Applicable Major 32.8%
Project based approach	N/A	N/A	N/A	N/A
Trainings	Applicable 50%	N/A	N/A	Applicable 14.2%
Extra assessments and controls	Applicable 25%	N/A	N/A	N/A
System Implementation	Applicable 25%	Applicable 100%	N/A	Applicable 14.2%
Client Consent	Applicable 100%	N/A	N/A	Applicable 85.7%
Data agreements with third parties	Applicable 25%	Applicable 100%	N/A	Applicable 28.5%
Review process	N/A	N/A	N/A	N/A

Table 13 Online Survey Outcome & Conclusions

4.3 Second Phase of Interviews

During the planning process of this research study, the idea of conducting a second round of interviews was estimated as a supplementary step for which we would need a couple more interviews in order to fill any research gaps that were not covered in the previous two phases. However, due to the restricted number of participants in the online survey, the number of interviews of the second round was extended from 3-4 interviewees to 7-8.

Also, considering the fact that from IT and Data Management representatives, there were only one from each, the aim for the second round was to find at least 3-4 specialists, heavily involved in relevant projects. Similarly, it was difficult to find contacts that have worked on PSD2 initiatives and therefore by this round of interview the target was to find 2-3 people specializing in this regulation.

4.3.1 Design of the second interview phase & objective

The ultimate goal of this round is, next to what mentioned just above about the diversity in the sample, to get some answers that were not clearly covered in the previous rounds and dive into more detail level. In particular the key topics addressed for further elaboration are:

-Training requirements, before and after the implementation

-DPIAs: review and continuous improvement

-IT implementations

-Maturity and further steps.

The table below summarizes the characteristics of the interview participants in regards to their position and professional background.

Interviewee Code	**Role**	**Seniority**	**Landscape**	**Background**	**Financial Services Domain**
D	Data Privacy Officer	Senior	Group Level	Finance	Wholesale Banking
E	Expert Consultant GDPR	Senior	Compliance	Finance, Economics	Cross-domain – Banking and Insurance
F	Data Privacy Officer/Data Protection Officer	Senior	Group Level	IT	General Banking Organization
G	Legal Counsel	Senior	Legal	Law	Cross-domain
H	Legal Counsel	Senior	Legal	Law	Wholesale banking
I	Program Manager for Change	Senior	Group Level	IT	General Banking Organization
J	Product Area Lead in Customer Data	Senior	Group Level	Financial Engineering ,IT	General Banking Organization

Table 14 Interview Round Two – Participants' Overview

4.3.2 Interview Conduct & Decoding Procedure

The second round, again due to Covid-19 pandemic situation, was conducted online by using tools such as MS Teams and Google Meet. All the sessions were recorded and transcribed (transcriptions can be found in the Appendix).

Decoding Steps

The method to follow in order to decode a qualitative analysis interview and get the relevant data out of it was conducted as per the steps defined below:

-Transcript the interviews.

-Read the transcripts as a whole (per interview) and keep notes, always considering the keywords.

-On each interview, start the labelling based on the keywords and phrases defined. For the labelling will take into account:

1. The number of times a word/phrase or synonym appears in the text.
2. Any words or phrases that have been highlighted explicitly by the interviewee as of high importance.
3. Any words of phrase that have been repeated in sources and articles, while conducting the literature review. Synonyms and phrases with similar meaning will be also included.

Definition of keywords

The table below consists of the keywords used for the decoding of the 2nd Phase of Interviews. This list below is derived from the main topics/subjects discussed but was also enriched after the interviews with some synonyms, expressions or phrases that could impact the outcome of the interview and the importance of it towards the research objectives. The keywords also are grouped under "Focus Topic", this grouping will be used in the next Chapter in order to summarize the overall results and define the proposed methodology.

4.3.3 Interview phase two outcome

The interview sessions were quite lengthy and extensive therefore it was important to set upfront the keywords and phrases that will be important for our research findings.

To start with, the decoding outcome is summarized in the tables provided in Appendix section 3.1 and 3.2. As mentioned before, the method used was focusing on compiling the number of times some key words are used and repeated during the interviews. The decoding was done per interviewee and then a total score per keyword was calculated.

As mentioned in the previous section, all keywords are grouped per Focus topics in order to facilitate the scope of our research questions.

To continue with the key outcome taken, let's describe how the analysis was done from the decoding phase to the outcome qualification.

4.3.3.1 Outcome for GDPR

The focus topics of our research were defined as such, Training, Impact, Process Assessment, IT implementation and Maturity.

The total number of times that a phrase or word was used, was calculated on word/phrase level. Therefore the results for each of them is the total sum of those numbers.

Diving into these numbers it is observed that the number of answers varies in the range of 0-16.This numbers will be used in calculations that are described in chapter 5 in order to classify the topics/aspects that will be qualified to our proposed process flow.

Keywords/Key phrases	**Additional words /Similar meaning**	**Focus Topic**	**Total per Keyword/phrase**
Change(s), heavy, impact, affect	Major, impactful	Impact	2
Continuously Learning sessions, continuous knowledge sessions, trainings	Course, seminars, constantly, repetitive, demand	Training	16
Multiple departments/disciplinary, jointly, together	Joint, different departments	Training	3
Awareness,aware, communication	Attention	Impact	13
In public, society		Impact	1
Mandatory course, mandatory e-learning	required, obligation	Training	6
Management supervision, control	Higher management/level, monitored	Training	5
Business Cases, incident analysis	practical examples/appliances, use cases	Training	3
PIAs, DPIAs, assessments, questionnaire	Questions	Process Assessment	9
On system, per system, on system level		Process Assessment	7
On process level, on data processes		Process Assessment	6
Revised PIAs, Revised DPIAs, (Re-)assessment, refine	update, change	Process Assessment	4
Yearly review, on yearly basis, every year		Process Assessment	1
GDPR proof, GDPR compliant	In order to comply	IT Implementation	0
System implementation, new system		IT Implementation	0
Legacy systems, old systems, issues		IT Implementation	3
Data sanitization, data minimization	Minimum required data	IT Implementation	1
Data encryption, anonymization	Anonymized data, masking, test	IT Implementation	6
Data Lake		IT Implementation	6
In control, Adequate level	Compliant, well, sufficient	Maturity	2

Maturity Levels	mature, advanced	Maturity	2
Not mature	insufficient	Maturity	1
BAU, integrated processes, integrated activities		Maturity	1
Obligation	follow, reactive	Maturity	3
Opportunities, Enable		Maturity	1
Further improvement, ongoing, in progress		Maturity	2

Table 15: Interview Round Two Outcome GDPR

The main conclusions are summarized as such:

Impact:

- Although there is no clear trend on the impact range of the regulation itself, GDPR attracted big attention in the society.

Trainings:

- Need for continuous education of the staff.
- Mandatory trainings to be in place.
- Joint contribution on the training material by different departments/ experts. Multidisciplinary approach is a plus.
- Need monitor mechanism preferably by higher management.
- Optimization of the training material by real-life examples, issue analysis or business cases can enhance the quality.

Process assessment:

- DPIAs were imposed by the regulation.
- The level on which the DPIAs are performed is either on processes or on IT systems.
- In some organizations they consider quite important the need of reviewing the DPIA procedure, comparing the current situation to the GDPR implementation phase.

IT implementation

- Data encryption methods were used to manage personal data.
- In concepts like data lakes, data masking was an additional exercise.
- In some cases, old legacy systems were excluded from GDPR related assessments due to future decommissioning.

Maturity

- Not clear trend about the current maturity situation.
- Evaluation outcome varies between being in control of being compliant and have achieved an advanced level of maturity.
- Continuous improvement focus can be considered.

4.3.3.2 Outcome for PSD2

The focus topics for PSD2 are: Training, IT implementation, Revised Guidelines, Competition & Maturity.

The way the decoding outcome was summarized is again similar to the one used for GDPR.

Keywords/Key phrases	Additional words /Similar meaning	Focus Topic	Total per keyword/phrase
Learning sessions, seminars, knowledge sessions	Course	Training	5
Not continuous trainings, limited need	not additional training, not broad	Training	7
Staff/Employees involved, specialists	Specific departments, lesser extent	Training	4
System implementation, new system		IT Implementation	0
API implementation, API in place	API based	IT Implementation	10
Revised guidelines, revised processes required, impact on API implementation	change, alter	Revised Guidelines	4
ICT requirements	technical, specifications, standards	Revised Guidelines	5
Customer Consent		Consent	0
Data Agreements with TTPs	One-sided consent	Consent	0
Market Competition	healthy competition	Competition	0
No Innovation Block	no disruption	Competition	1
Adequate, in control		Maturity	1
Not adequate		Maturity	1
BAU, integrated processes, integrated activities, mature	embedded	Maturity	4
Further improvement, ongoing, in progress		Maturity	0

Table 16 Interview Round Two Outcome PSD2

Similarly, the main conclusions are summarized as such:

Training:

- Limited to specialists involved directly in PSD2 related activities
- No need for re-occurring sessions.

IT implementation

- Imperative to open up data access via APIs.

Consent:

- Topic not covered by the second interview round, however covered in the online survey and its importance is quite impactful.

Revised Guidelines

- The publication of the revised guidelines was quite impactful.
- The organizations had to reassess the new ICT requirements and relaunch their APIs.

Competition

- No clear trend on how PSD2 enhances market competition.

Maturity

- Not clear trend about the current maturity situation.
- The relevant processes have been embedded in the daily way of working.

5. Overall Outcome & Proposed Methodology

In chapter 5, considering the outcome of the phases describing above and compiling the results collected, we are going to define a process flow with all the requirements that banking organizations need to meet in order to comply with the regulations. The requirements will be also classified based on the level of mandate that was defined during the research phase; there will be mandatory steps as well as suggested assessments or solutions that the organizations have implemented in order to enhance and facilitate the compliance purposes.

5.1 Overall Outcome from Interview round two & online survey

Our research phase was split into three rounds, interview round one, online survey and interview round two. Because the first round was limited to three interviewees and it was exploratory, it will not be considered explicitly into the methodology calculations. The outcome of that round has been used in formulating the questionnaire of the survey, therefore not extra analysis is required.

Focusing on phase two and three, for each phase we have identified the key topics of the research focus; in order to specify the outcome for fitting our research purpose, it was important to identify the dimensions to be used for the suggested calculations. The dimensions are defined as per below:

1. Importance: as defined by the person conducting the research or the potential impact on the research objectives.
2. Frequency: defined considering how often the subject was highlighted by the interviewees or survey participants. For the interview results, the frequency will be calculated as the percentage of on how many interviews it has been mentioned out of the total number of interviews executed on the specific regulations. For example, for interviews that the focus was only on PSD2, those will be excluded from the total when we focus on GDPR related calculations. For the survey results, the frequency has been calculated on the total number of answers.

3. Expertise factor: considering the demographics of the participants in terms of their professional experience, expertise background and seniority in the related GDPR/PSD2 involvement.

The table below depicts the factor percentages as defined for the importance factor as well as by the person conducting the research.

Factor	Category	Percentages	Reasoning
Low	Importance	0.25	
Medium	Importance	0.55	
High	Importance	0.95	
Finance, Economics	Background	0.75	FI scope
Legal/Compliance	Background	0.60	Regulatory mandate
IT/Data Management	Background	0.75	IT implementation requirements - complexity
Cross - Domain	FI Domain	0.90	Diverse experience – wider insight
Wholesale Banking	FI Domain	0.60	Wholesale domain limitation
General Banking	FI Domain	0.85	Wider insight
Retail Banking	FI Domain	0.60	Retail domain limitation
Other	FI Domain	0.60	

Table 17: Table with defined weight values

At this point it is important to mention that the backgrounds of the participants are slightly different from the ones we used in the grouping while analysing the survey results. From survey backgrounds the Finance/Economics background is missing. Those participants are included in the category “Other” where external consultants and advisors were counted as well.

In order to be able to apply the suggested formula, we need to compile the outcome results of the online survey and the second interview round. The outcome of the survey will be incorporated to the outcome of the interview round.

From the topics covered in the online survey, ones that could be matched on the final list of keywords and keyphrases have been incorporated in the latest list. On the tables below both the Frequency and the Incorporated to fields have been added, for both GDPR and PSD2 outcome tables.

GDPR key words/ phrases	Legal/Compliance 4P	IT 1p	Data management/control 1p.	Other 7p	Frequency	Incorporated to
Comparison to predecessor regulation	Applicable Major Impact	Applicable Major Impact	Applicable Major Impact	Applicable Major Impact 71.4%	0,846	Changes, Heavy ,impact(ful)
Project based approach	N/A	N/A	N/A	N/A	N/A	N/A
Training afore	Applicable 50%	Applicable	Applicable	Applicable 14.2%	N/A	N/A

Training after	Applicable	Applicable	Applicable	Applicable 71.4%	0,923	Mandatory course, mandatory e-learning
Internal roles clearly defined and assigned	Applicable 50%	Applicable	Applicable	Applicable 71.4%	N/A	N/A
Client consent	Applicable 75%	N/A	Applicable	Applicable 71.4%	N/A	N/A
Data Agreements with third parties	N/A	N/A	N/A	N/A	N/A	N/A
DPIAs on system level	Applicable 25%	Applicable	Applicable	Applicable 28.5%	0,308	On system, per system, on system level
DPIAs on process level	Applicable 75%	N/A	N/A	N/A	0,231	On process level, on data processes
Review of DPIAs	N/A	N/A	N/A	N/A	N/A	N/A
System Implementation	Applicable 75%	Applicable	Applicable	Applicable 37.5%	0,615	System implementation, new system
Maturity in control, adequate*	Applicable 25%	N/A	Applicable	Applicable 71.4%	0,539	In control, Adequate level
Maturity Optimized**	Applicable 75%	Applicable	N/A	Applicable 28.5%	0,462	Opportunities, Enable

Table 18 Incorporation of Survey Key outcome in keywords table for GDPR

PSD2 subject					Frequency	Integrated to
Comparison to PSD1	Applicable	Applicable	Applicable	Applicable	N/A	
	Major 50%	Neutral	Neutral	Major 32.8%		
Project based approach	N/A	N/A	N/A	N/A	N/A	
Trainings	Applicable 50%	N/A	N/A	Applicable 14.2%	0,231	Not continuous trainings, limited need
Extra assessments and controls	Applicable 25%	N/A	N/A	N/A	N/A	
System Implementation	Applicable 25%	Applicable	N/A	Applicable 14.2%	0,231	System implementatio n, new system
Client Consent	Applicable	N/A	N/A	Applicable 85.7%	N/A	
Data agreements with third parties	Applicable 25%	Applicable	N/A	Applicable 28.5%	N/A	
Review process	N/A	N/A	N/A	N/A	N/A	

Table 19 Incorporation of Survey Key outcome in keywords table for PSD2

5.2 Proposed Methodology

The objective of this research study is to define the process steps that banking organizations need to follow, considering the regulatory and technical requirements, in order to comply with GDPR and PSD2. During our research, we ran into a lot of discussions on how the organizations have struggled with specific aspects like the consent or the internal processes, how they managed to overcome those and by which means/methods.

While working on the specific process steps we need to decide which requirements/assessments are mandatory to be included, or less important but also some that have been crucial and contributed to quick wins. In order to come up with this sort of classification we will use the below formula. This formula will be applied on keyword/ key phrases level.

5.2.1 Suggested Formula

In order to define a way to classify the process requirements we need to follow a calculation that includes all the factors to take into consideration.

In particular, the total weight will be calculated as the Sum of the weights of interview phase and the weights out of the survey.

Each weight is equal to the multiply of Importance X Frequency X the median of Expertise Factor

Total Weight Formula = $\underline{\sum \textit{(Importance X Frequency X Median(Expertise Factor))}_{\textit{interview+Survey}}}$

The values used for the calculations on the tables below, are the ones defined in Table 17. The final expertise factors were calculated as per below:

Final Expertise Factor GDPR = Background X FI Domain X Expertise Factor GDPR

Final Expertise Factor PSD2 = Background X FI Domain X Expertise Factor PSD2

For the expertise factor we will use the Median value as:

Median= (exp.fac1+exp.fac2+…..+exp.facn)/n

The reason behind using the median value of the expertise factors, is the relatively wide spread of the values. In particular, we see in Table 20 and Table 21 ,the distribution of the values and therefore the best method to approach it is to take the median of its values and get the most central values of the sample. The two graphs following are giving the overall picture of the value distribution.

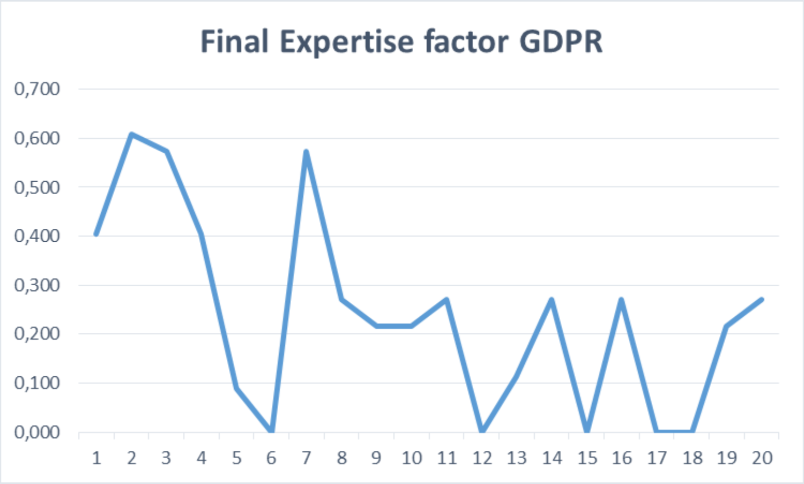


Figure 16: Distribution of values for GPDR Expertise Factors

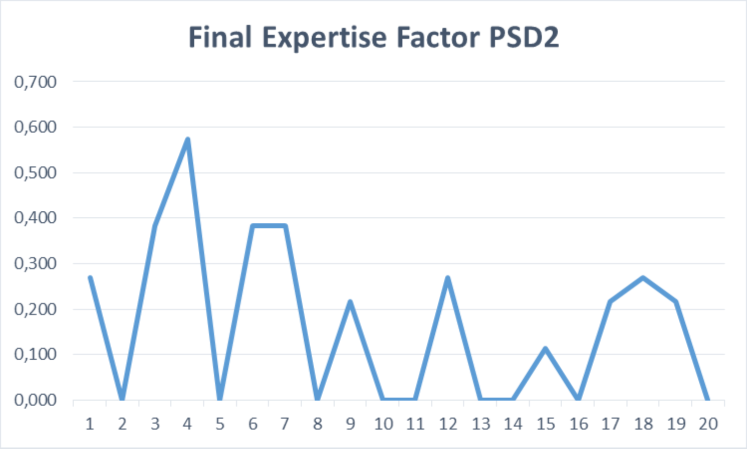


Figure 17 Distribution of values for PSD2 Expertise factors

For both the interview and the survey sections the expertise factors are defined as such:

Code	**Role**	**Background**	**Financial Services Domain**	**Expertise GDPR**	**Expertise PSD2**	**Final Expertise factor GDPR**	**Final Expertise Factor PSD2**
D	Data Privacy Officer	0,75	0,60	0,90	0,60	0,405	0,270
E	Expert Consultant GDPR	0,75	0,90	0,90	N/A	0,608	N/A
F	Data Privacy Officer/Data Protection Officer	0,75	0,85	0,90	0,60	0,574	0,383
G	Legal Counsel	0,75	0,90	0,60	0,85	0,405	0,574
H	Legal Counsel	0,60	0,60	0,25	N/A	0,090	N/A
I	Program Manager for Change	0,75	0,85	N/A	0,60	N/A	0,383

J	Product Area Lead in Customer Data	0,75	0,85	0,90	0,60	0,574	0,383

Table 20 Expertise Factor Calculations for Interview Phase Two

Code	Background	Financial Services Domain	Expertise factor GDPR*	Expertise Factor PSD2*	Final Expertise Factor GDPR	Final Expertise Factor PSD2
1	0,75	0,6	0,6	N/A	0,27	N/A
2	0,6	0,6	0,6	0,6	0,216	0,216
3	0,6	0,6	0,6	N/A	0,216	N/A
4	0,75	0,6	0,6	N/A	0,27	N/A
5	0,75	0,6	N/A	0,6	N/A	0,27
6	0,75	0,6	0,25	N/A	0,1125	N/A
7	0,75	0,6	0,6	N/A	0,27	N/A
8	0,75	0,6	N/A	0,25	N/A	0,1125
9	0,75	0,6	0,6	N/A	0,27	N/A
10	0,6	0,6	N/A	0,6	N/A	0,216
11	0,75	0,6	N/A	0,6	N/A	0,27
12	0,6	0,6	0,6	0,6	0,216	0,216
13	0,75	0,6	0,6	N/A	0,27	N/A

Table 21 Expertise Factor Calculations for Online Survey Participants

The survey Expertise Factors are defined as such:

Median Final GDPR Exp. Factor = 0.27

Median Final PSD2 Exp. Factor = 0.216

At this point is it important to mention that for the survey participants, the expertise factors per regulation were considered based on the answers given on the questions in regards to trainings attended and most importantly whether the respondents have been participated in project or activities directly related to those regulations. (Questions 5, 6, 12, 19, 20, 22)

Based on the outcome of the Total Weight calculation, the key topics will be classified as such:

Total Weight Formula outcome	Classification
> 0.75	To be included in the suggested process as best practice
<= 0.75 && >=0.30	To be included in the suggested process as preferred practice
< 0.30	To be excluded from the suggested process

Table 22 Classification per Total Weight Table

5.2.2 Calculations and Conclusions

Considering the factors described above, next step was to calculate the weights based on the suggested formula. The detailed calculations are included in the Appendix 4.1 and 4.2, where the weight outcome is sorted from the highest value to the lowest.

Example

One example of the formula calculation:

For Training category, in regards to the Mandatory Course/E-learnings, the Total Weight is:

Interview (Frequency X Importance X Median (Expertise Factor)) + Survey (Frequency X Importance X Median (Expertise Factor)) =

(5/6 X 1 X Median (0.405,0.574, 0.405 , 0.09, 0.574)) + (0.923 X 1 X Median (0.27, 0.27, 0.216, 0.216, 0.1125, 0.27, 0.27, 0.216, 0.27)) =

(5/6 X 0.41) + (0.923 X 0.27) = 0.34 + 0.25 = **0.59**

Total Weight is equal to 0.59, value between 0.75 and 0.30, which classifies it as preferred practice.

Outcome and Conclusions

After applying the suggested formula, the top weights qualified to be part of the suggested GDPR process only as preferred practices. There were no values exceeding 0.75. The rest of the calculations gave weights less than 0.30, therefore they will be excluded from the final process.

Keywords/Key phrases GDPR	**Additional words /Similar meaning**	**Focus Topic**	**Total**
Mandatory course, mandatory e-learning	Required, obligation	Training	0,59
PIAs, DPIAs, assessments, questionnaire	Questions	Process Assessment	0,38
Awareness, aware, communication	Attention	Impact	0,34
On process level, on data processes		Process Assessment	0,33
Change(s), heavy, impact, affect	Major, impactful	Impact	0,30

Table 23 GDPR Total Weight Outcome Table

The conclusions of the previous phase of the research need to be redefined after the calculations. In particular:

Impact:

- The new publication of GDPR could be considered impactful, driven by the fact that it caught wide attention publicly.

Trainings:

- The GDPR related trainings have become mandatory among the organizations.

Process Assessment:

- DPIAs preferably to be performed on the processes related to data management activities.

IT implementation:

- Not specific data sanitization method followed, methods varies per organization.
- Not specific data masking activities executed.

Maturity:

- Not clear outcome on where the banking organizations stand in terms of maturity.

Similarly, below there are the relevant weights qualified to be included in the PSD2 process, as preferred choices.

Keywords/Key phrases PSD2	**Additional words /Similar meaning**	**Focus Topic**	**Total**
API implementation, API in place	API based	IT Implementation	0,38
Not continuous trainings, limited need	not additional training, not broad	Training	0,36

Table 24 PSD2 Total Weight Outcome Table

The relevant conclusions for PSD2 topics are:

Training:

- The need for continuous learning is very limited.

IT Implementation:

- APIs to be in place and open up to TTPs.

Consent:

- Not clear outcome on how impactful it was.

Revised Guidelines:

- Redefined ICT guidelines by EBA. Not clear outcome on the impact volume.

Competition:

- No contribution observed on enhancing the market competition

Maturity:

- Not clear outcome on where the banking organizations stand in terms of maturity.

5.3 Limitations & Sensitivity Analysis

5.3.1 Research Limitations

Geographical

The starting point of our research was the review of the regulations, the scope of which is extended to all EU member states and covers any financial services organization, especially for PSD2. The scope of our project is limited to banking organizations in the Netherlands. Although the observations taken, from the literature review as well as from surveys and interviews, show that the main actions taken and processes adjusted to the new standards, can be applicable in different countries and financial organization, there is still a risk that those practices might differ per country.

Therefore, the survey and interview data would be interesting to be enriched with input from other countries like Belgium, Germany or France but also from other types of financial services organizations. However, our sample of experts working in Dutch banking services met our initial requirements considering the scope and the reliability of the outcome is not questionable; highlighting that the experts interviewed have worked in the three biggest Dutch banks, ING, Rabobank and ABN AMRO, with some of those experienced in more than one of these banks.

Participants Sample Size & Background

For all the phases of our research, interview phase one and two and online survey, the target number of participants was higher than the one achieved. In particular, the initial estimation for the online questionnaire participants was 20-25, but the achieved number of people filling it in, is 13. For the first round of interviews, the estimated sample was 5 participants, but the achieved one was 3. Similarly for the second round, the aim was 8-10 interviewees but the round was finalized with 7 interviews. All the phases lasted longer than initially anticipated due to the lack of finding experts available, using business and university network as well as online means like LinkedIn.

In addition, to the limited number that participated in the research phases, it is important to mention that although it was achieved to find people from different backgrounds within the FIs, their experience with GDPR and PSD2 related projects and initiatives, were not always as extensive as expected. Although, we used the expertise factor to capture this inefficiency, it is still risky to consider the outcome fully representative.

5.3.2 Sensitivity Analysis

Because of the limitations described above, we consider important to perform a data driven investigation in order to observe any changes or trends as if the sample is closer to our initial estimations.

5.3.2.1 Sensitivity Analysis GDPR

This assessment will be performed by examining the behaviour of the suggested formula while the expertise factor values are fluctuating to meet our initial estimations. The method of sensitivity analysis is selected for that purpose, as it determines the impact that independent variables could have on dependent ones [27]. It is most known as “What if…” analysis; giving an example in our study:

“What would be the total weight if the expertise factor was increased by 15%?”

In order to have reliable results we will perform this assessment based on different scenarios.

Scenario 1: For the second round of interviews, the median of Final Expertise Factor is 0.49. What if we increase the GDPR Expertise Factor for Interviews D, G, H (where the values are smaller compared to the median) to be equal to the median value? With this scenario we want to examine what would happen if the audience's expertise was focused on GDPR and the values wouldn't vary much from the median.

Interviewee Code	Role	Background	Financial Services Domain	Expertise GDPR	Final Expertise factor GDPR
D	Data Privacy Officer	0,75	0,60	0,90	~~0,405~~ 0.49
E	Expert Consultant GDPR	0,75	0,90	0,90	0,608
F	Data Privacy Officer/Data Protection Officer	0,75	0,85	0,90	0,574
G	Legal Counsel	0,75	0,90	0,60	~~0,405~~ 0.49
H	Legal Counsel	0,60	0,60	0,25	~~0,090~~ 0.49
I	Program Manager for Change	0,75	0,85	N/A	N/A
J	Product Area Lead in Customer Data	0,75	0,85	0,90	0,574

Table 25 Scenario 1: Final Expertise Factor GDPR adjusted for interview 2nd phase

The detailed calculations can be found in the Appendix 5.1. Based on the total weight outcome the below keywords are qualified (Table 6.4)

Scenario 2: For the second round of interviews, what if all the participants were GDPR experts, therefore the GDPR Expertise Factor to be 0.90 (the maximum value applied). The values have been adjusted for Interviewees G & H. With this scenario we aim to proof that if more GDPR experts were participating the impact on the final outcome could be quite important.

Interviewee Code	Role	Background	Financial Services Domain	Expertise GDPR	Final Expertise factor GDPR
D	Data Privacy Officer	0,75	0,60	0,90	0,405
E	Expert Consultant GDPR	0,75	0,90	0,90	0,608
F	Data Privacy Officer/Data Protection Officer	0,75	0,85	0,90	0,574
G	Legal Counsel	0,75	0,90	**0,90**	**0,608**
H	Legal Counsel	0,60	0,60	**0,90**	**0,324**
I	Program Manager for Change	0,75	0,85	N/A	N/A
J	Product Area Lead in	0,75	0,85	0,90	0,574

	Customer Data				

Table 26 Scenario 2: Expertise Factor GDPR for interview 2nd round

The detailed calculations can be found in the Appendix 5.2. Based on the total weight outcome the below keywords are qualified (Table 27)

Scenario 3: For the online survey the median of Final GDPR Expertise Factor is 0.27 while for the Interview Round two is 0.49. What if we increase the median of the survey final factor to 0.38 (median (0.27, 0.49) = 0.38. With that scenario we increase the expertise in the survey participants by giving a value equal to the median value for expertise of our total sample.

The detailed calculations can be found in the Appendix 5.3. Based on the total weight outcome the below keywords are qualified (Table 27)

Scenario 4: For all the participants in the survey and interview round, we will remove the background and Financial services factors, and therefore the Final Expertise Factor for GDPR would be equal to Expertise Factor GDPR. By that scenario we aim to see what if we only consider the sample's participation in GDPR related activities, no matter the type of organization they work for and their department.

The detailed calculations as well as the updated table of expertise factor calculations can be found in the Appendix 5.4. Based on the total weight outcome the below keywords are qualified.

Observations

The Table 27 below summarizes the fluctuations of the Total Weights per scenario applied.

Scenario 1: By increasing the expertise in the Interview phase and have the values concentrated closer to the median value, we see quite an increase in some topics but still the same keywords are qualified to be included in the process, yet as preferred practices.

Scenario 2: For the less experienced in GDPR interviewees, we increased the expertise factor to 0.90 as if they were experts too. By that we consider that the total population of this interview round are GDPR specialists therefore more targeted audience. Also, a maturity component is qualified to be considered in our final approach.

Scenario 3: The participants of the online survey were 13 but also not experts in both regulations. Therefore, by this scenario we increased the GDPR expertise factor to be equal to the median 0.38. By that we consider the participant's expertise quite adequate to be part of our research sample. In addition, two more components are qualified to be included in our suggested process, maturity and process assessment related.

Scenario 4: By removing the Background and FI type expertise factors, we only take into account the GDPR experience of the participants in related projects, no matter if they are legal, IT or data experts. By that we consider equality on the background and their importance on the contribution to relevant activities. Also, we anticipate that the way of managing personal data and implementing GDPR is not differentiating based on the type of bank. The outcome of the new calculations gives some switches on two subjects to exceed 0.75 and become best practices, while a couple more are qualified to be preferred rather than conditional.

Keywords/Key phrases GDPR	Additional words /Similar meaning	Focus Topic	Total	Total Scenario 1	Total Scenario 2	Total Scenario 3	Total Scenario 4
Mandatory course, mandatory e-learning	Required, obligation	Training	0,59	0,66	0,73	0,69	1,30
PIAs, DPIAs, assessments, questionnaire	Questions	Process Assessment	0,38	0,38	0,38	0,38	0,60
Awareness, aware, communication	Attention	Impact	0,34	0,41	0,48	0,34	0,75
On process level, on data processes		Process Assessment	0,33	0,33	0,33	0,35	0,55
Change(s), heavy, impact, affect	Major, impactful	Impact	0,30	0,31	0,33	0,39	0,61
In Control, Adequate Level	Compliant, well, sufficient	Maturity	N/A	N/A	0,30	0,32	0,54
On system, per system, on system level		Process Assessment	N/A	N/A	N/A	0,30	0,48
System implementation, new system		IT implementation	N/A	N/A	N/A	N/A	0,37
Revised PIAs, Revised DPIAs, (Re-)assessment, refine	Update, change	Process Assessment	N/A	N/A	N/A	N/A	0,34
Opportunities, Enable		Maturity	N/A	N/A	N/A	N/A	0,32
Maturity Levels	Mature Advances	Maturity	N/A	N/A	N/A	N/A	0,30

Table 27 Outcome of Sensitivity Analysis for GDPR Scenario 1,2,3 & 4

5.3.2.2 Sensitivity Analysis PSD2

We continue with PSD2, by applying the same logic as in the sensitivity analysis for GDPR.

We will use the following three scenarios:

Scenario 1: For the interview second round, what if all the participants were PSD2 experts, therefore the PSD2 Expertise Factor to be 0.85 (the maximum value applied). The values have been adjusted for Interviewees D, F, I and J. With this scenario we aim to proof that if more PSD2 experts were participating in the interview sessions, the final outcome could be quite closer and more reliable based on our initial estimations. Final Expertise Factors are updated accordingly.

Interviewee Code	Role	Background	Financial Services Domain	Expertise PSD2	Final Expertise Factor PSD2
D	Data Privacy Officer	0,75	0,60	~~0,60~~ – 0,85	~~0,270~~ – 0,383
E	Expert Consultant GDPR	0,75	0,90	N/A	N/A
F	Data Privacy Officer/Data Protection Officer	0,75	0,85	~~0,60~~ – 0,85	~~0,383~~ – 0,542
G	Legal Counsel	0,75	0,90	0,85	0,574
H	Legal Counsel	0,60	0,60	N/A	N/A
I	Program Manager for Change	0,75	0,85	~~0,60~~ – 0,85	~~0,383~~ – 0,542
J	Product Area Lead in Customer Data	0,75	0,85	~~0,60~~ – 0,85	~~0,383~~ – 0,542

Table 28 Scenario 1: PSD2 Expertise Factor for interview 2nd round

Scenario 2: For the online survey the median of Final PSD2 Expertise Factor is 0.22 while for the Interview Round two is 0.54. What if we increase the median of the survey final factor to 0.38 (median (0.22, 0.54) = 0.38. With that scenario we increase the expertise in the survey participants by giving a value equal to the median value for expertise of our total sample.

Scenario 3: For all the participants in the survey and interview round, the background and Financial services factors are excluded from the calculations, and therefore the Final Expertise Factor for PSD2 would be equal to Expertise Factor PSD2. By that scenario we aim to see what if we only consider the sample's participation in PSD2 related activities, no matter the type of organization they work for and their department/ position.

The detailed calculations can be found in the Appendix 5.5, 5.6 and 5.7 for Scenarios 1,2 and 3 retrospectively. The outcome is summarized in Table 29.

Observations

Scenario 1: Because of the lack of PSD2 expert interviewees, we increased the expertise factor to 0.85 as if they were all experts. By that we consider that the total population of this interview round are PSD2 specialists therefore more targeted audience based on our initial estimations. Although we see some increases in the subject's weights we do not see major changes, the same topics to be included plus one training component.

Scenario 2: The participants of the online survey were limited to 13 but also not experts in both regulations. Therefore, by this scenario we increased the PSD2 expertise factor to be equal to the median 0.38. By that we consider the participant's expertise quite adequate to be part of our research sample.

Scenario 3: By removing the Background and FI type expertise factors, we only take into account the PSD2 experience of the participants in related projects. By that we consider equality on the background and their importance on the contribution to relevant activities. Also, we anticipate that PSD2 regulation is not differentiating based on the type of bank; the main principles and assessments are applicable in any banking sector. We see a couple of new components to be qualified in the process, but also a switch, one from preferred to best practice.

Keywords/Key phrases PSD2	Additional words /Similar meaning	Focus Topic	Total	Total Scenario 1	Total Scenario 2	Total Scenario 3
API implementation, API in place	API based	IT Implementation	0,383	0,542	0,394	0,60
Not continuous trainings, limited need	not additional training, not broad	Training	0,356	0,483	0,383	1,08
Staff/Employees involved, specialists	Specific departments, lesser extent	Training	N/A	0,325	N/A	0,36
System Implementation		IT Implementation	N/A	N/A	N/A	0,6

Table 29 Outcome of Sensitivity Analysis for PSD2 Scenario 1,2 and 3

6. Conclusions

6.1 Conclusion on research questions

The main question as it was stated at the beginning of our research: *How the data landscape needs to be reformed in financial services organizations in order to comply with the new regulations of GDPR and PSD2?*

The current research study aims to define how the recent publications of GDPR and PSD2 in 2019 have impacted the way the banking organizations are managing personal data. The scope of our research covers the requirements that the banks have to fulfil in terms of processes, systems and data handling, and how they can reach the adequate levels of maturity in order to be compliant. Some of the requirements are imposed by the regulators and therefore there will be defined as obligations in the suggested process.

The table summarizes the key topics and requirements:

ID	Regulation	Requirement	Type
1	GDPR	Define data related roles and responsibilities	Regulatory obligation
2	GDPR	Assign Data Privacy Officers	Regulatory obligation
3	GDPR	DPIAs	Regulatory obligation
4	GDPR	DPIAs on process level	Preferred practice
5	GDPR	DPIAs on system level	Conditional practice

6	GDPR	Mandatory Learnings	Preferred practice
7	GDPR	Review of DPIAs	Regulatory obligation
8	GDPR	Data Minimization	Regulatory obligation
9	GDPR	Data Sanitization	Conditional practice
10	GDPR	Customer Consent Explicit	Regulatory obligation
11	PSD2	APIs accessible to TTPs	Regulatory obligation
12	PSD2	Learnings limited to staff involved	Preferred practice
13	PSD2	Customer Consent between TTPs	Regulatory obligation
14	PSD2	ICT & Security reporting	Regulatory obligation
15	PSD2	Revised ICT & Security reporting	Regulatory obligation
16	GDPR/PSD2	EU & National Supervision	Regulatory obligation

Table 30 Key requirements for the suggested GDPR and PSD2 Process Flows

6.2 Suggested process flow GDPR

Considering the outcome of the all research phases described above, our aim is to propose a process flow that bank organizations have to follow to become GRPR compliant. There is a number of actors defined for this process, who are either external, such as EU regulators, European and Local Supervisors and internal, such as the Legal and Compliance employees, the Finance/Business representatives and the IT departments. In addition to those we add the Customers because the customer consent topic is crucial for GDPR.

To continue with, the suggested flow is divided in four phases, considering also the sequence of the requirements and the applied steps. The description of the process will be performed on phase approach:

- Publication Phase: The trigger of the whole process is the publication of GDPR regulation by EU authorities. The detailed regulation articles where published in the official websites of EU, also available in different official languages. At this phase, both the EU Data Supervisory Authorities and the local ones have to review the regulation and the requirements and also contribute on any additional guidelines that are crucial for the implementation. Next to them, the internal legal and compliance employees have to review and understand the new requirements and accordingly relate those to the needs of the banks. The role of the Data Protection Officer (DPO) is included in this group of actors, because the role is now imposed by the regulation and it is very significant both for supervising and reviewing activities.
- Pre-implementation Phase: This phase is important for the organizations, they have to define and allocate the relevant roles because they will be crucial in order to move with the implementations required. It is also responsibility of the legal/compliance councils, together with the DPO to develop the new data policies and standards and provide guidelines to assist the rest of the organization to understand what is required and then be able to translate it into strategy. The development of the strategy is a joint activity where contribution is required from both the business and IT organizations. Business is driving the requirements and IT is responsible for providing the IT solutions that will help the whole organization to meet the GDPR obligations. The IT solutions are either system requirements or data management ones. It is common that a project or programme is formulated where the representatives from all necessary angles of the bank are now dedicated to GDPR implementation activities. Moreover, due to the dimensions that GDPR publication had taken and the importance of having explicit customer consent in order banks to be able to manage sensitive personal data, the reach-out campaign to customers to get informed and request their consent, had taken place before the go live date. Only if the customer give the

consent the bank can include his/her personal data in their systems and keep managing it. To finish with this phase, there was big demand on training the bank employees on what GDPR is bringing; not only for the staff to be involved in GDPR tasks but to the organization as a whole. Therefore, the trainings provided have to be really precise and concise, fact that required a cross-functional approach from the trainers.

- Implementation Phase: During this phase, the new ways of working that the regulations have imposed are taking place. One of the most important ones is the performance of DPIAs which is now an obligation. Although there were guidelines published for the DPIAs, each organization had to adjust it on their needs and tools and therefore the preferred practices qualified are to be either on system or on process level. After all the relevant IT roll-outs have to take place. Most of the implementations had to deal with applying data minimization methods on data management systems, as one of the main principles of GDPR. Next to that, some other IT solutions have been driven by reassessing the access right principles on legacy systems or using some anonymization or masking techniques on the data itself. In regards to the need of trainings, they have become mandatory but also preferably they need to occur on continuous basis, considering how the organizations are progressing on their remediation of reporting incidents.

  Before moving to the aftercare phase, it is important to highlight the importance of the supervision, both the EU and country authorities had to supervise and review the reports provided by the banking organizations. Internally, within the organizations it is clearly the DPO to guarantee that everything is under control.
- After Care Phase: As after care we consider any action that needs to be re-occurring such as review of the policies and standards by DPO. But also, in case there is a new update or revision of the regulation, the bank organizations they need to perform the same actions like review of the regulations articles, translate into their needs and accordingly take care of any new implementation on the IT side.

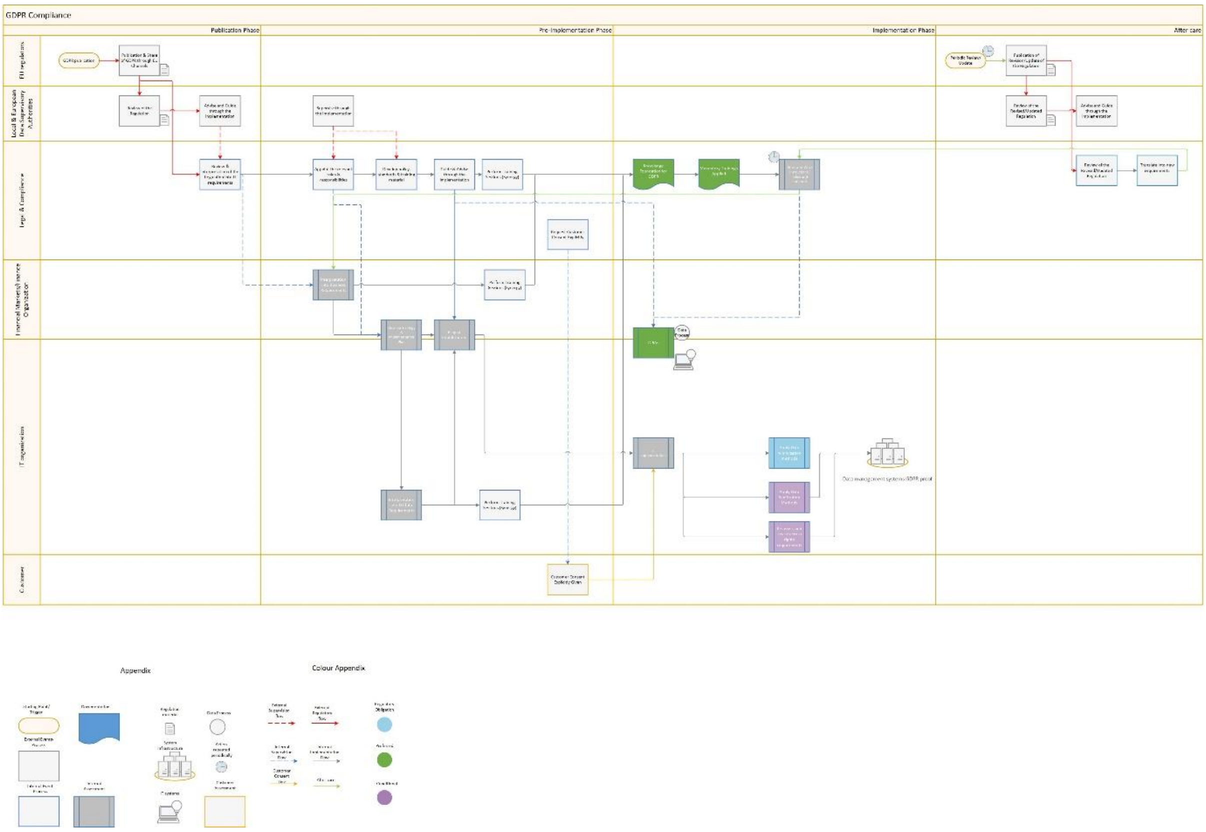

GDPR Compliance
Publication Phase
Pre-Implementation Phase
Implementation Phase
After care
EU regulators
Local & European Data Supervisory Authorities
Lega & Compliance
Financial Markets/Finance Organization
IT organization
Customer
GDPR publication
Publication & Share of GDPR through EU Channels
Review of the Regulation
Advise and Guide through the Implementation
Supervise through the implementation
Appoint the relevant roles & responsibilities
Develop policy, standards & training material
Data management systems GDPR proof
Appendix
Colour Appendix
Starting Point/ Trigger
Documentation
External Events Process
System infrastructure
Data Process
Action required periodically
Systems
Internal Assessment
Regulatory Obligation
External Supervision flow
External Regulations flow
Customer Consent flow

Figure 18: Process flow suggested for GDPR compliance.

6.3 Suggested process flow PSD2

The PSD2 suggested flow has been designed using the same logic as for the GDPR one. In PSD2, the actors involved are also defined as internal and external and they are again the EU regulators, European and Local Supervisors, the legal and compliance counsellors together with financial markets and IT representatives, and the customer. The description of the process will be done on phase basis, in order to cover also the sequence of the steps performed.

- Publication Phase: The trigger of the process is the publication of PSD2 regulation by EU authorities. The detailed regulation articles where published in the official websites of EU, also available in different official languages. At this phase, both the EU Data Supervisory Authorities and the local ones have to review the regulation and the requirements and also contribute on any additional guidelines that are crucial for the implementation. Considering the impact of the ICT and Security Guidelines later in the process, it is important to highlight the first publication of those was in 2018. Internally, the legal and compliance employees have to review and understand the new requirements and accordingly translate them into the needs of the banks.
- Pre-implementation Phase: This phase is important for the organizations, they have to define and allocate the relevant roles, and especially the DPO role who is responsible for supervising the implementation but also to guarantee the relevant documentation is in place. The development of the PSD2 strategy is a joint activity where contribution is required from both the business and IT organizations. Business is bringing the requirements and IT is responsible for translating into PSD2 proof solutions. For PSD2 it was imposed that the banks should open their APIs to the TTPs to gain access. No other significant impacts have been identified in the systems. The consent topic is now on TTPs responsibility to get it from the customer. To finish with this phase, the need for trainings was limited only to the employees

directly involved in PSD2 projects, not widely among the whole organizations. However, it had to be a joint effort from experts coming from different backgrounds in the banks.

- Implementation Phase: The APIs were already in place for the organizations, what they had to do to be PSD2 compliant is to re-adjust the control of the access to them. That was done by applying Identity controls and certificate requirements so that the TTPs are granted the relevant access.
- New Revised ICT Requirements: This is more an event rather than a phase; because of complaints and issues on the ICT and security reporting, the EBA was obliged to publish new revised guidelines. This event triggered a chain of actions quite impactful for the organizations. New requirement had to be fulfilled and also the controls of opening up the APIs to be reviewed. As a result the organizations had to review the new guidelines and again reintroduce the APIs to the TTPs.
- After care Phase: As after care we consider any action that needs to be done on a regular basis such as the review of the policies and standards. But also, in case there is a new update or revision of the regulation, the bank organizations they need to perform the same actions like review of the regulations articles, translate into their needs and accordingly take care of any new implementation on the IT side.

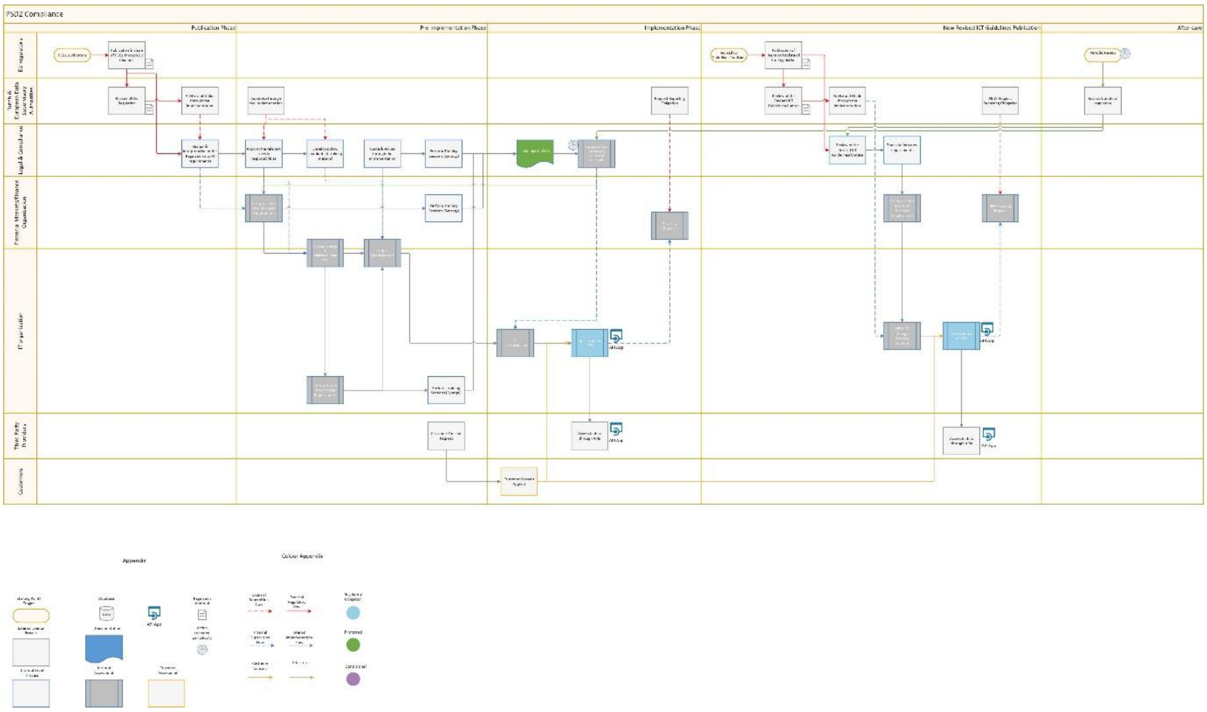


Figure 19: Process flow suggested for PSD2 compliance

7.Reflections & Future Work

7.1 Reflections

After providing the research conclusions and the suggested processes, there is some field for reflection on the way this research study was conducted. In particular there are two dimensions on this research to reconsider:

-The research approach: At the research design phase, the sequence of the research steps was defined. After the literature review, the goal was to have an exploratory round of interviews and then continue with the online questionnaire and the second round of interviews. Considering now the outcome of both the interview rounds and the survey, especially of the low number of participants, I would have scheduled some steps differently. An alternative approach could have been to have conducted a more extensive interview round at the second phase (8-10 interviewees) and also use those contacts for the online survey after. By interviewing more experts at the beginning, we could come up with the key topics at the earlier stage and adjust the questions in the survey in a more targeted way. Also, those experts could have been a means of forwarding the survey to their peers in GDPR and PSD2 projects and therefore potentially we could get more participants.

-The weight calculation formula: the way of performing the outcome analysis of interviews and survey imposed to apply some formula on how the key subjects/activities can be included or not in a suggested process for the organizations to follow. While envisioning this formula and discussing with the supervisors, the idea came up to use an X factor that could contribute to more targeted results. For that purpose the idea of the Expertise Factor was introduced for the participants in our research and it was defined as such:

$$\text{Expertise Factor}_{\text{GDPR/PSD2}} = \text{Background X FI domain X Expertise Factor}_{\text{GDPR/PSD2}}$$

At this point of reflection and always considering the sensitivity analysis performed on section 5.3.2, I would have only considered the extent of the participants' participation in dedicated GDPR and PSD2 actions and not their background and their banking sector. It is observed that in the sample of participants, the number of dedicated experts to the regulations was quite restricted. There were also some interviewees with limited experienced on both regulations or having being involved only in wholesale activities versus retail. For all those reasons, the expertise factor instead of providing concrete picture of best practices, it was eliminating the scores and as a result we did not come up with best practices as initially anticipated. The components included in our suggested processes were only qualified as preferred or conditional ones.

7.2 Future Work

The nature of this research study leaves quite some field for further work. The suggested processes were designed considering the current situation in the Netherlands and within banking organizations. Further work could contribute on providing a more concrete process, mainly composed of best practices rather than limitations to preferred solutions or optional ones.

-Future research could be conducted on different types of Financial Institutions such as Insurance Companies, Asset Managers or Pension Funds. It would be interesting to test whether those practices can be applied in a similar way, the challenges along the implementations and what kind of data sanitization methods could be used.

-Future research could also be expanded in a wider scope among the EU countries. The Dutch banks are quite wealthy and robust, supporting the robust financial system in the Netherlands. Also, this country is ranked quite high in innovative IT solutions which could also support their banking technology needs. By expanding the scope in other countries, with less stable financial systems such as in Greece or Portugal, it could give a different approach on how difficult their banking organizations could implement GDPR or PSD2 solutions, taking into account the maturity of their services and the costs.

References

[1]: “Chapter 3: Critically Reviewing the Literature”: Research Methods for Business Students, 5th Edition (2009), *M. Saunders- Ph. Lewis- A. Thornhill*

[2]: “What is personal data”: GDPR, Data protection published by European Commission

[3]: “General Data Protection Regulation (GDPR), Article 1 Subject matter and objectives” https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

[4]: “What is GDPR, the EU’s new data protection law?” http://gdpr.eu

[5]: “Data Controller vs. Data Processor: What is the difference? “ August 2020, *Chris Brook*

[6]: “General Data Protection Regulation (GDPR), Article 5 Principles related to processing of personal data” https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

[7]: “General Data Protection Regulation (GDPR), Article 7 Conditions for consent” https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

[8]: “General Data Protection Regulation (GDPR), Article 25 Data protection by design and by default” https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

[9]: “Data protection by design and default”, Guide to GDPR, Information Commissioner’s Office UK

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/

[10]: ”Tasks and powers of the Dutch DPA” Autoriteit Persoonsgegevens

https://autoriteitpersoonsgegevens.nl/en/about-dutch-dpa/tasks-and-powers-dutch-dpa

[11]: “Chapter 13: Analysing qualitative data”: Research Methods for Business Students, 5th Edition (2009), M. Saunders- Ph. Lewis- A. Thornhill

[12]: “Directive (EU) 2015/2366 on EU-wide payment services, Summary of the directive” https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32015L2366

[13]: “PSD2; Payments >Rights and Obligations” published by De Nederladsche Bank https://www.dnb.nl/en/payments/psd2/rechten-en-plichten/index.jsp

[14]: “PSD2; Payments >New services” published by De Nederlandsche Bank https://www.dnb.nl/en/payments/psd2/nieuwe-diensten/index.jsp

[15]: “How banks can balance GDPR and PSD2” published by EY ,February 2019, *J. van der Kroft, P. Kuijsten*

[16]: “PSD2; Payments >Supervision” published by De Nederlandsche Bank

https://www.dnb.nl/en/payments/psd2/toezicht/index.jsp#!faq-tcm:47-371452

[17]: “General Data Protection Regulation (GDPR), Article 35 – Data Protection Impact Assessment

https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

[18]: “General Data Protection Regulation (GDPR), Article 9 - Processing of special categories of personal data https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

[19]: “Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679” published by European Commission

[20]: “Everything you need to know about PSD2” published by BBVA October 2019

https://www.bbva.com/en/everything-need-know-psd2/

[21]: “Supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards on the criteria for appointing central contact points within the field of payment services and on the functions of those central contact points” published by European Commission in 14th March 2019

[22]: “PSD2, GDPR and Banking Secrecy: What Role for Consent?” Written by Sebastiao Barros Vale, June 2019

https://www.lexology.com/library/detail.aspx?g=09534fc1-7f28-46c6-a7cb-20574fefe9de

[23]: “Payment Services Directive 2 for FinTech Payment Service Providers” by EY/HVG Law, June 2018

[24]: “What has changed since PSD1”, by Stevens & Bolton, B. Flynn, G. Duhs ,L. Stewart, 2019

[25]: “Final Report on Guidelines on ICT and Security Risk Management” By EBA, 2019

https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/872936/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management.pdf

[26]:”Final Report, Revised Guidelines on major incident reporting under PSD2” By EBA, June 2021

[27]: Sensitivity Analysis definition

[28]: “CMMI – An introduction to capability model integration”

https://www.bmc.com/blogs/cmmi-capability-maturity-model-integration/

Appendix:

1. Additional definitions & Abbreviations

RASCI Model – Responsibility Assignment Template

R	Responsible
A	Accountable
S	Supportive
C	Consulted
I	Informed

Useful Abbreviations

GDPR	General Data Protection Regulation
PSD2	Payment Services Directive 2
PSD1	First Payment Services Directive
EBA	European Banking Authority
API	Application Program Interface
AISP	Account information service providers
PISP	Payment initiation service providers
TPPs	Third Party Providers
BAU	Business as usual
ICT	Information and Communications Technology
DORA	EU legislative proposal for an EU regulatory framework on digital operational resilience

Capability Maturity Model Integration (CMMI) – The levels of maturity used in the survey questions are based on the CMMI classification; this model is quite popular among business organizations.

Level 1	Initial – Organizations lack in planning, lack in integrated processes, not able to make decisions
Level 2	Managed – Planning and some processes in place, part of business objectives can be met. The organizations are reactive to the changes imposed by the regulations.
Level 3	Defined – Processes of level 2 are improved, well documented and monitoring mechanisms are in place. The organizations can now be more proactive.
Level 4	Quantitatively Managed – the planning, processes and monitoring mechanisms of level 3 are progressing and they can be measured and conform to official metrics and KPIs.
Level 5	Optimized – Continuous improvements of the aspects mentioned on level 4 and innovative solutions introduced.

2. Interviews' Transcriptions

2.1 First phase

Interviewee A

Question 1: "As a consultant it is expected to provide advisory services to multiple clients. In GDPR, the main roles defined are those of controller, processor and third parties of processing. Do you service clients from the whole role scope? "

Answer 1: "The majority of the projects involved for GDPR is for data controller contribution. What we initially focus on is to get the understanding of the processes like for example to an HR department, based on the process we define the legal ground and the purpose of the process; when on-boarding new employees we define the beginning and the end of the processing activity and also the purpose.

Question 2: "With regards to the processing part, the controller imposes the rules and the purpose of data collection, and the processors are diving more on the system level of handling data. Is there a sort of consent? Not only from a client perspective but also from an internal clause."

Answer 2: The starting point is always to initiate a conversation with the department that assesses the data. Of course taking into account whether it is the controller or the processor, or maybe both. The process of identifying what is done should be similar for processors and controllers. When performing an assessment and want to understand the data processing activity and the type of data used through it, what is the legal ground and the purpose, not always in scope to check the contracts if the employee/consumer gives already his consent for that specific situation. It might be applied but that is not the standard approach.

Question 3: "The HR example is more of a case of a new party entering a new organization. What about to a different department like the one handling client data information, how is there a consent mechanism applied? Do you do an assessment like PIA on system and data level? "

Answer 3: "There are two approaches when we talk about PIAs;

- First approach is based on assets such as IT system infrastructure, where a PIA is performed per IT system to get an understanding of the personal data in the system but also the processes and the ground and purposes.
- Second approach is to consider processing activities/ processes so as to dive into specific steps of those process tasks.

Question 3.1: " What is observed so far in Bank A is that we perform PIA on system level, by filling-in some questionnaires and that assessment generates a classification whether the system contains personal data or not. But also we dive on a deeper level, actually on the data level. Do you propose something similar? To perform an assessment per data field/item?

Answer 3.1: "That is possible, but need to take into account when we talk about assessments it really differs per type of client. For example, in a bank it is a very different and sophisticated environment of systems, data and the infrastructure around. At smaller organizations it seems easier to perform these assessments; at the beginning of the project to make a structure to be followed and predefined but in the case of the bank it is more logical to begin from the system level and dive in the data. The challenge of looking at data level is when there are many systems, where there is a lot of information. Its challenging then to define the purpose of the usage of the data that can be used from one system but for multiple purposes."

Question 3.2: "The complexity of the system infrastructure and the flow of data among different systems in Bank A, imposed the assessment on data level. There is a classification whether the data are personal data sensitive, transaction sensitive and economic sensitive."

Answer 3.2: "That indeed can be a possible approach but there is no 100% direction from the local authorities on working methodologies. A bank approach might not be applicable to different types of industry."

Question 4: “Going back to the assessment approaches, would like to elaborate more on the processing steps of question 3”

Answer 4: “On Asset level typically the starting point is to get an understanding on the type of assets in the organization. Get an overview of all assets and next step go to one of the applications where to identify the purpose of using this application and the type of data used in it and how the data flow. Important to define what kind of data is stored and/or edited in the system. After that you can move to the DPIA assessment where you can answer the critical question about the IT systems.”

Question 4.1: “In a more complex data landscape, when the data flows from one system to the other. How would you dive in this case? Would you go for a solution to track by performing data lineage from E-2-E flow, and then have a holistic view? Or is it preferable to perform it on each and every system separately?”

Answer 4.1: “Would go individually do the analysis per system, but the connection point should be taken into consideration especially for changes on the flows between systems. The overview should be there. There are multiple ways to do that, but the connection point should be in place.”

Question 4.2: “Coming back to previous question, about the purpose that an application is used for, the kind of data used and how they flow. Are there specific processing actions like write, overwrite, delete etc. Do you dive into detail for the actions or limit the analysis on the purpose, origin and destination of the data?”

Answer 4.2: “Going for the second option. Need to be very strict in the beginning to define the purpose of the whole exercise. You can always go deeper on details but that can lead to lengthy and never ending process. If you ensure you get the required information, make it feasible when you set the goal and the strategy of the process.”

Question 5: “Does it also happen that you consult a third party that is processing data on behalf of a controller?”

Answer 5: “Third parties need to be included in the overview, need to know their role in the whole process. Even for third parties it is important, but if the third party is outsourcing to another third always there is risk. But we do not contact third parties, we mitigate the risk by having data protection agreements between the responsible organizations and third parties. When the assessment is performed, all those parties and it should be mitigated by DPIAs.

Question 6: “Do you use specific ways or frameworks for data anonymization?”

Answer 6:” There are some methodologies developed by the consultancy firm. For those methodologies we get input from local authorities per country but also industry platforms like International Security Forum, ISO standards. Standards from the market are used to compile the methodology.”

Question 7: “When it comes to having a client sending data outside of the EU like clients in the US. Do you need extra clauses or consent for the usage of the data?”

Answer 7: “We do service global clients; it brings extra requirements or obligations with them. It could be multiple and make it complex with local requirements.

Question 8: “Do you use specific concepts in the data landscape? Concepts like the data lake or moving from the traditional Databases to Data Marts? Or like the data lake which gets popular lately but seems challenging for GDPR compliance”

Answer 8: “We do not have a standard method to use but indeed there are different solutions. We do look critically at those concepts.”

Answer 9: “Do you see any kind of trend? For example retail companies follow specific solutions compared to wholesale or banking organizations? Looking for a match between the industry and the nature of the business and the possible solution?”

Answer 9: “We do have market specific approaches; my focus is on financials”

Interviewee B

Question 1: “What were the main changes GDPR brought compared to previous data privacy regulations?”

Answer 1: “Compared to the previous law, the Dutch law on the protection of personal data, GDPR did not bring that many changes in how to deal with personal data. It just took it to a European uniform level and raised major attention on the protection of personal data. If you wanted to declare that you were in control already, you should have complied with the previous law like seven or eight years ago. Even now these days we come across with people saying “You don’t comply with GDPR”. No, you are not complying with the predecessor of GDPR, instead of running 2 years behind you should run 8 years behind. Content wise GDPR did not bring that many changes to the protection of data, but it raised awareness among consumers about the importance of the protection of their personal data. That is the main change in Europe and that also comes from the desire from the European Union to have better consumer protection laws. If you look at all the laws and regulations that have been coming towards us from the EU the last few years, many of them are targeting a better protection of consumers.

Question 2: “Based on what you just described, it was a sequence of actions inherited from the previous law. Because GDPR is really precise with the roles and the responsibilities around each role and of course the silent consent situation, how did you reach those specific requirements?”

Answer 2: “Well, of course in the approach of GDPR in 2017 none saw that coming, raising awareness among Bank X and Bank X realized that we need to do more. So, the function came into effect, we appointed a Chief of Privacy or Chief of Data Protection, and after some assessments followed on how to implement GDPR. At a certain point we can say I should have done this or that, but now is a good timing to have it all in one programme. So with the approach of GDPR in 2019, there was a worldwide programme for the implementation of GDPR and to assure that all the elements of GDPR are implemented. Only after the closing of the programme it was assessed that it was primarily based on retail of Bank X Netherlands. The scope has not been sufficiently estimated towards Wholesale and Rural and the regions outside of Europe. When we talk about GDPR everyone thinks about Europe only. All over the world, in Australia, in South America, even in China, everybody is making new privacy laws and regulations and most of them are modelled in a way that they mirror GDPR. First we have the GDPR programme, then we discovered this is too much retail based, wholesale insufficiently in the scope and then they designed a global programme GDPR 2 to sufficiently incorporate wholesale as well. Retail was then out of scope of the deliverables of Programme 2. So GDPR 2 focused on wholesale and regions outside Europe and it is finishing in the end of March 2021. Now we have new insights, we now see that the global programme is so advanced that it brings wholesale on the next level. Now retail is looking again at the deliverables and continuously growing. About functions, a global protection officer was appointed and privacy officer, there is also a privacy committee that is a sub-committee of the global Risk Management Committee, and this committee is mandated to discuss risk privacy among the organization. There is quite good structure and governance to make sure we are in control in the privacy subject. Now, we try to bring the privacy elements to the first line, second line was compliance and risk management. When we have the transfer to the business as usual, that is now ongoing, we see that a lot of topics are transferred to the responsibility of the first line.

Question 3: “Going back to the roles, we have the data controller, the data processor and we might have also third parties. Which department is acting like a data controller to set all the requirements of the purpose of the data? Is there a specific team?”

Answer 3: “We have now a very difficult topic. For Bank X the controller has not been established. On the lowest level like processes and systems, we say that the system owner determines the purposing of ownership. Hence for that system the system owner is the controller and he should make sure that the system fulfils all the requirements, is compliant to GDPR and that there is data processing agreement with the processors and that we do PIA, so privacy statement for that system and your customers. But when we build that up, when we aggregate we need a controller on Bank X level like on the Board of Directors. We have the

Global Privacy Committee where the Privacy Executives of all domains is in chair. We have around 10 domains (like retail, wholesale, CIO, COO etc.) in the privacy committee. All these executives are gathered and the act as a controller of Bank X Group. Whenever we have a domain overarching or a global issue, then we address that to the committee as a joint controller and make sure you have the relevant element or issue addressed within Bank X.

Question 4: “Then the assessing of the data would go to the system users like data processors who are doing extract, edit, deletion or any action around data.”

Answer 4: “We are the controller. The data processor is the 3rd party.”

Question 5: “Does Bank X has third parties to process data?”

Answer 5: “A lot; for example on payments, Bank X sells you a card but as soon as you buy something in a shop there is processor who executes the transaction for us. We determine the purposes, the means and the goals and they process it for us. The system owner of Europe Payments (who involves a processor), he should do the PIA on the processing and then also determine the conditions for our contract.

Question 6: “Then we have to sign DPAs with them right?”

Answer 6:” Yes, sometimes we have a data transfer, usually within Bank X, and we have a Data Processing Agreement when we transfer data to Third Parties. For example Schrems is all about privacy, Facebook was sharing personal data with US third parties, violating European Laws. That also requires Bank X to rethink all of our data transfers to the US”

Question 7: “Coming back again to the third parties, before GDPR, guess there were still agreements on how they would treat data, for which purposes etc. but what we all noticed when GDPR went live officially, we have been receiving emails from multiple organizations like “we fall under GDPR you have to give your consent from now on for us to use your data. So, how was that exercise for Bank X? ”

Answer 7: “It wasn’t, because believe that consent is not the right legal base for processing personal data. Consent is only used by controllers who cannot think of a better legal base to process their data. If anyone asks for consent you should question “why do you ask for consent, don’t you have a legal base? Are you doing something that is on the edge of legitimacy?” We have 6 legal bases on the GDPR, of which 3 apply: 1. legitimate interest 2. Compliance with law 3. Performance of a contract. Bank X does not ask for consent because we believe that consent is the wrong signal to clients as we cannot think of any better legal base. Consent gives you so much hassle that you can give consent one day and withdraw it the next day. We need to have a real-time system that monitors when consent has been given, withdrawn, given again etc. Within Bank X we say don’t process personal data based on consent. The privacy laws don’t say anything about you cannot do. They say if you want to do this, then you should fulfil these obligations. So if you want to do something legitimate with personal data you don’t have to ask for permission. Therefore you have to mention it on the Privacy Statement: I am processing your data for these specific legal bases, purpose etc. ”

Question 8: “Switching our discussion to more tangible deliverables; do you do anything with PIAs? I see from the regulation itself, there is a very detailed document with the guidelines and I tried to create a matrix with roles and actions and where the DPO roles lies in it. So you have to advise on the requirements but also keep an eye on the progress, if there is a deviation of the agreed process. Could you elaborate on that topic?”

Answer 8: “We have in Bank X a system called Collibra, where we ask for all processes, systems and other processing activities, we ask the system owner to perform a PIA. We split it in two phases; first data inventory which like a quick scan and reveals risky types of processing personal data, then you need to go to the risk assessment. In the risk assessment, they elaborate on the risk mitigating measures taken if still needs to go on with this processing. When that is done in the first line by the process or system owner, then you are assisted by compliance advisor of your department on checking the results of the inventory and the data assessment. If they agree this is properly reflecting what is going on and the risk properly mitigated then via Collibra this is sent to Global Privacy Office. Every risk assessment is only applicable is there is any risk spotted, if not then only data inventory phase is needed. So when there is a risk assessment in place, the Global Privacy Office needs to have an opinion whether the identification of the risks is alright, and that the risk mitigation measures taken are sufficient. They can even approve or reject, but in any case after discussion with the system owner and the compliance advisor."

Question 9: "After the completion of the assessment, is there a generation of classification (like A, B, C) depending on the type of data that each system contains?"

Answer 9: "No, that is done on the data inventory; there are some questions of risk triggers and if those are triggered you need to go to the risk assessment if not then no assessment required, inventory is enough."

Question 10: "The risk assessment is also in Collibra?"

Answer 10: "Yes, that is the second stage of the PIA process. Every system owner has to fulfil a lot more actions of obligations. In CMDB that is the global system for all systems so other classifications need to be performed too or assessment. AIC (Availability – Integrity –Confidentiality) assessment. There is a threshold for example if it is 1-1-1 then you get low risk compared to 2-2-3. In the assessment of those systems it also determines rules like above a specific threshold you have to perform a PIA as well. Next to the obligation of course that if you process personal data you have to conduct a PIA. There multiple triggers towards performing a PIA but also multiple ways to assess the risks of the system involved. But there is not a direct connections saying from AIC classification to Risk classification for PIA. The privacy risks are detected in PIA itself "

Question 11:" Going a bit deeper on data level, I know there is some assessment whether data are personal data, transaction or economic data sensitive. I guess that is done on the data inventory phase?"

Answer 11:" The first question of the data inventory is "Does this system process any personal data? " If the answer is no then you can stop, if the answer is yes then you move on. There is also questions like "Do you process personal data of children, any sensitive personal data and indeed transaction data and so on. " There is a breakdown of all the elements that are in the law and there also triggers about the risk in order to go to the risk assessment.

Question 12: "I think I need to dive in the DIQ, because I got information mainly from the PIA itself on the system level."

Answer 12: "In Collibra you can find the PIA but you can also try a dummy one to see how the flow goes."

Question 13: "Going to the PSD2, the way of raising awareness was going hand-to-hand between GDPR and PSD2. There is a lot of article and analyses whether there is an overlap on the requirements. PSD2 focus on the transactional line and not on the personal data. So, you deal a lot with GDPR, does also PSD2 falls under your territory?"

Answer 13: "I will give you a contact person to help you on PSD2. What I know for PSD2 there is the possibility of account information services. There are third parties that give you as a consumer an overview of all your bank accounts within different banks. Those parties deal with personal data so we are very hesitant to open up our books to those parties because we don't know about their level of security. We only interact with those third parties via APIs. At the same time, there is a German company called Sofort AG who provide account information services but they also ask to let them manage bank accounts. What you have to do then as a consumer is handover the credentials of your account. Even if you wanted that as a consumer, like take over my account and responsibilities, in the general conditions of every account of every bank, it says you can never give your credentials to anyone. There is an interesting crossing between GDPR and PSD2, better elaborate with PSD2 colleague."

Question 14: "How often do you review the PIAs and the inventory? "

Answer 14: "Do not know the exact rules for that, at least once in every three years but of course for the most risky systems it can be done once in one or two years. Do not know if it is automatically determined, but once you enter your system assessment in Collibra, you finish PIA and risk assessment, then it is defined whether review needed in a year or three. Maybe you can find it in the Global Standard Privacy by Design for specific type of system.”

Interviewee C

Question 1: “I see that your role within Bank X organization sits in IT domain with focus on transactions. How are you involved in PSD2 related activities?”

Answer 1: “Indeed my position is in the IT side. I am involved in PSD2 because of transactional data requirements. My background comes from finance before.”

Question 2: “How would you comment on the comparison between PSD2 and the former regulation?”

Answer 2:”Among our environment the changes did not bring a big impact. The former regulation was already known.”

Question 3: “What was the reaction of Bank X to the new regulation? There were related projects formulated?”

Answer 3: “Exactly, a new project has been created for PSD2. I got a role there as a Program Manager.”

Question 4: “Would you say that the impact of implementing such regulation was big enough to affect multiple domains of the organization? Especially due to the subject of the client consent”

Answer 4: “The matter of the consent should not be considered as something new. I mean someone being a customer should be trusting the organization managing his personal data. Why should an extra consent should be given? By signing a contract you are supposed to show trust.”

Question 4a: “Were there in place any trainings before the implementation of PDS2?”

Answer 4a: “Yes, there were provided to the employees that their everyday work has been impacted by the new law.”

Question 5: “Do you see a relation between the PSD2 regulation and GDPR? Do you agree with the statement that both regulations are built on the same basis, the one of the client consent?”

Answer 5: “At a first glance you could say that indeed the consent subject is common let’s say, but in practice the requirements for GDPR are more specifically described and the purpose of the data usage is mandatory to be signed.”

Question 6: “What were the main actions taken in the PSD2 project? “

Answer 6: “Within the IT infrastructure there were some assessments in order to make sure the processes there were compliant to the new regulation. From system perspective some extra controls have been implemented to make sure the relevant employees have the relevant access to the systems.”

Question 6a: “Has that affected the way Bank X was providing data to third parties?”

Answer 6a: “ Yes but not drastically. As said before some additional controls and restrictions were sufficient to adjust our systems and make them compliant.

Question 7: “Would you face any complaints or reaction from customers in regards to the way the bank is managing their personal data? Do you see hesitation?”

Answer 7: “Although I am not a front-office employee, I would say that the new regulation didn’t change much on the customer side. For example for GDPR the organizations were obliged in May 2018 to send relevant emails about the new law, the purpose of managing data and informing the clients. For PSD2 purposes, we see that there adjustments made on DPA level, between the organizations and Third parties, no direct consent from the client was always necessary. "

Question 8: "At this moment we talk (April 2021) does the PSD2 project exist? Or you could say things have been brought on BAU level?"

Answer 8: "The project does not exist anymore. The relevant departments and employees have been now switched their way working accordingly."

Question 8a: "how do you monitor at the moment the compliance levels to the PSD2 regulations? I know for example that for GDPR there is a re-occurring visit on the requirements and on the PIAs. Is there something similar in place for PSD2 purposes?

Answer 8a: "By making our systems PSD2 proof and by enhancing our agreements with Third Parties, we manage to have a compliant process. Internally, we have our internal risk and control framework and on a yearly basis we audit the process. I hope that this does answer your question."

2.2 Second Phase

Interviewee D

Question 1:" Our first topic to cover today will be the training-learning sessions. Before or close to the implementation of GDPR there were relevant trainings provided. How do you stand today in regards to that topic, do you still provide trainings?"

Answer 1: "We still try to organize something that draws the attention to privacy or use articles. We have a quiz and a webinar and I think in April there was the World Privacy Day or World Data Protection day, something like that, when we are taking the opportunity to get attention on the privacy topic. So there is a foundation and then there is repetitive communication every year, every month, whatever. So yes we do provide some form of continuous training"

Question 2: "Coming back to the mandatory concept, you said there are some people who say "I am busy and I cannot attend" and other stuff, did you monitor that everyone had done that training or through the knowledge tier of foundation you can monitor that?"

Answer 2: "No, there was a privacy program that was run worldwide. The attendance of employees was mandatory and was also monitored and reported. So there were reports on how many people had attended and there were signed-off by management on the fulfilment on the training obligations. For the continuous mandatory trainings, so every year we have to go through a refresher and that's mandatory as well. And that's also monitored and reported on. So if I don't remember, Let's say I have to do a training by the end of next month, I get a reminder and my manager is going to call and say "Hey you have to do this training" , so there is definitely monitoring on all mandatory trainings."

Question 2a:" Alright, I think that was it for the training."

Answer 2a: "We have to show that all our people are trained. I think that Article 5 says something about organizational and technical measures. We think training and awareness is an organizational matter to show that you comply with GDPR."

Question 3: "That were mainly my questions about the trainings and the sessions. So, moving on I would like to address a topic like, I know there were some projects to make systems that manage data, GDPR proof, for example Filenet. Have you been involved in this kind of projects or are you aware of those?"

Answer 3: "Well, we have identified the need for tooling. Because let's say, handling data breaches, we cannot do that in Excel anymore. You cannot just have an excel sheet and write something down. So we have put proper tooling to handle data breaches. We also have identified the need for tooling, for what we call legal watch or legal compliance so, in order to identify worldwide the data privacy legislation and then to make sure that you are compliant. Because we see we have GDPR in Europe but now we have LDP in Brazil and the Chinese privacy law and all the states in the United States they have separate privacy laws. We need some kind of system, some kind of tooling to first alert us on new legislation and then for us to be able to identify all the requirements and log our compliance to all those requirements. So now we are in the process of buying the proper tooling for legal compliance. Let's say for privacy by design we have to perform the PIA process right? And if you are in a risky processing you have the mandatory PIA to be performed. We also have a system for that, we have a system that you can have, call it data inventory questionnaire and also risk assessment. And that is connected to the administration of systems and processes, so we have an administration of all the systems. So all the systems in the systems database must have a PIA as well. Of course that is the ideal state, so we are working towards the ideal state as you understand what I mean?"

Question 3a: "yeah, and that is connected to something like the control framework of the processes?"

Answer 3a: "No, there is a difference between CMDB and Collibra. So if you randomly pick a number of systems and you to check both in the systems database and in Collibra, whether they are in and whether they are properly assessed. And then we do a quality qualitative assessment whether the answers to the questions are the correct answers. So, yes indeed there is a connection with the risk control framework as well."

Question 4:" I guess there were also some changes in relation to the record keeping or the retention policy right? Like handling personal data and having GDPR implemented, I know that there is retention policy in the banks on how long they are keeping personal data. There was also a revision of these policies because of the new regulations?"

Answer 4:" We, in the privacy office or in the DPO groups, are not the owners of the record keeping theme. Record keeping is not our responsibility but we did participate in record keeping program to make sure that let's say privacy requirements were also incorporated. Because record keeping says (privacy legislation says) do not store for so long. But record keeping requirements have both: not storing too long but not too short, cause if you store too short you cannot have an audit trail or you cannot fulfil tax obligations. Thus mainly we have to keep records too old.

Question 5: " Ok that is about the retention policy of personal data or contracts, your role is similar. You participate but you are not having the ownership of the process.

Answer 5: "We brought the privacy requirements into the record keeping program. From a privacy perspective we always say do not store for too long, but from other laws or legislations it says you should store at minimum for 5 or 7 or 20 years. So that's all in the retention/record keeping policy."

Question 6:" Do you know if there is a different in the handling of historic data? Like the data used to run some models or predictions. Was that also covered by this worldwide program?"

Answer 6:" Good question. Usually we are more concerned about not using live data. We often get questions on data modelling and algorithms or whatever we call test sets. Then we need the data sets to test. Then we say Ok, as long as you are not testing with live data. Then we can be pretty Ok and rather anonymize, have a method instead of personal data.

Question 6a: "So, I guess you are using methods like anonymization or pseudonymization?"

Answer 6a:" You know, I would rather have metadata so you know one layer above. And the thing is we often get questions of that, and then if you talk to those people and ask them the right questions, as why do you really need this and that information. And sometimes they say we don't really need that. But then it really does not contribute to the goal they try to achieve and then they say if you take that out, there's no personal data so you have no problem. So, it's also a matter of consulting people on what is a good thing to do. We always say: GDPR doesn't say easy. GDPR says proportionate and necessary, so if it's not strictly necessary, then don't process any personal data please.

Question 7:” Another activity, of course we have external providers that they are handling data on behalf of the banks. You said you are investing now on having the proper tooling, in order to be proof of those regulations. But the transfer of data, how has been affected so far?

Answer 7:”Mostly Scherms, are you aware of that? The complaint filed against Facebook. Everybody in Europe, every company in Europe processing personal data, is now looking at a way to transfer personal data outside the EU and especially to the USA in proper manner. Because the transfer mechanism is invalid, we no longer have the privacy shield and the safe harbour. So Bank X is running a major program on data transfers and especially data transfers to our own non adequate countries. And we are trying to come up, just as every other company in Europe, to come up with a solution on what standard contractual clauses we need to have, to be able to transfer personal data. So, the topic of transfer personal data and that is intertwined with what we call vendor management and outsourcing and that kind of stuff. So yes that is a topic in motion, we are working on it. We have also said that in the meantime no new transfer personal data to non-adequate countries can be initiated. It’s about two weeks ago period.”

Question 8:” I guess the way you are doing the PIAs is still the same like you did. Because now the regulation is there for three years and more. Have you changed anything in the way you are conducting the PIAs? ”

Answer 8:” Well, we keep finding PIAs questions. The first model of the PIA questions was a first attempt and since then we keep refining the PIAs questions. And we keep adding guidance. Let’s say only due to missed interest assessments. If you use a legitimate interest as a legal basis, then you have to perform a legitimate interest assessment. Now we have recently come up with a template to weigh the interests and to administer debt and we also added the DT (data transfer impact analysis), so as soon as you come to the topic of outsourcing or data transfer on top of the PIA, you now have to perform a data transfer impact assessment, all because of that Schrems ruling. So we keep refining our privacy by design tools and templates.”

Question 9:” So I guess it’s a continuous process improvement. Going to the next question. What do you think it can have been done differently? From your experience while implementing this kind of initiatives for GDPR. Do you think at this moment are you satisfied with the maturity? Have you reached the basics that are enough to comply with the regulation or there are some points to improve?”

Answer 9:” We can stand the test of the regulators. If the privacy authorities or the privacy regulators are coming to us for audit, maybe they are not going to say it’s a perfect 10, but we are definitely in control. And yes we need to need to enhance some features but if I look at the environment, if I look at the society, then I think in general that the financial institutions are doing pretty well regarding the privacy, because are used to handle confidential client data and this is not similar, but it is in the same field as privacy. So you know from a historic perspective we are used to handling sensitive personal data of client right. GDPR is just a formalization of what we have been doing already with client data. So, I am not saying we are mature, but I think we are in control. We are aware of our obligations and we are to the largest extend compliant. There will be topics to enhance if I look at others on the commercial environment and what they are doing with personal data, it is not at the spirit of the law. And with others I mean commercial, marketing data. All kinds of commercial enterprises, gambling houses, outside of the financial sector. Well if I compare us to them, we are pretty mature. And because we are running the global privacy program, we have at least insured some basic compliance to the GDPR and all worldwide privacy legislations. I am not too worried about compliance. That is also what we see from the complaints that we get. We asked functionally mailboxes and as a client you can either go to your banker or you can address it to the local branch of your city, but you can also write an email directly to the DPO. The complaints or the questions we are getting in the DPO mailbox..People tagged them as privacy complaints but 90% are not privacy complaints, there are about general dissatisfaction about something else. And because we have this functional mailbox that they can address, they say you are violating my privacy. Then we look at the question and it’s not about privacy. So that also indicates to us that from privacy perspective we are not doing that bad, doing pretty ok.”

Question 10:” Do you think that the principles of GDPR, as said at the beginning of this call, were considered that we have to comply, have to avoid the risk of paying fees, risk of reputation. Do you think that some of those can be enabled on opportunities, and they can be welcomed more optimistically treated in the companies?"

Answer 10: "Definitely, I mean ranking is trust, so being a client of the bank is mainly about trusting the bank to handle your data. And then, only recently the whole concept of personal data has come up by means of privacy legislation. But for hundreds of years, banking has been about trust. Trust the bank with your data first, with your money and then with your data about you. So I think GDPR as privacy legislation is not threat, it's just another building block in building trust at our clients. Being GDPR compliant is another manner showing to our clients that we are really careful with their data. Most people they don't care about the difference between data, financial data or personal data. It's all in the same ballpark. As a bank, being serious about GDPR is another opportunity towards clients to say we are careful with your data and personal data. Within the company, it's an opportunity from the Privacy Office to say that privacy is important, look at the law, we need to have more attention for the personal data so being backed up by the law. It's a good manner in the privacy office to have some power in the company. Privacy is important; the newspapers is all for privacy. There is daily newsfeed about privacy violations, fines and complaints, so it's good for awareness. I always say that the possible fines, are not a reason to be careful with personal data. The only reason to be careful with the personal data is because you value your clients and you want to keep their trust."

Question 11:"At this point we can say that many of the activities have been transferred from project phase to BAU, and in the meantime you are implementing your tools. Any other actions?" That's a summary of where we stand now.

Answer 11:" definitely."

Question 12:" Are you aware that last June, by the European Authority, they launched revised guidelines under PSD2?"

Answer 12:"There is a clash in between of what GDPR (or at least data protection authorities say) versus what the PSD2 rulebook says. It's called APIs and it's about the technical connection between the bank and the third parties. There is the technical rulebook that says something about the interface and the manner in which we have to transfer the personal data. The privacy providers claim that is not good enough; not according to privacy and PSD duty. The rulebook says something completely opposite; there is a big clash between privacy supervisors and the PSD rulebook.

Question 12a: "Are you aware of any actions taken by Bank X side?"

Answer 12a:" Bank X, together with all other banks in the Netherlands, formulated a community to address that issue. Together with D&B (the Netherlands Central Bank) which is the supervisor of PSD2 and the pricing authority to sort it out. So, the combined Dutch banks have addressed this topic to the representative supervisors.

Question 12b: "So now you are more on the waiting mode to see how far can go with this?"

Answer 12b: "Using the technical specifications that the Dutch privacy regulator says it is not good, we are in a squeeze here."

Question 12c:" You addressed that as all banks united, do you think that is also affecting the market completion?"

Answer 12c:" The technical standards should be change, if that is the answer. The technical requirements are not about blocking competition or about trying to prevent us from transferring data to payment services providers. It's about meeting the requirements of the Dutch Privacy Authorities and these authorities said We had everything in place, we can do it tomorrow. We have APIs in place, technical infrastructure and all of a sudden the regulator says we cannot do it. So we are just trying to meet requirements and not block any competition."

Interviewee E

Question 1:" I know that you work as a consultant with experience in many different companies. Can you describe what kind of positions did you have in personal data related projects?"

Answer 1: "At first it was project management and then data governance & data analysis roles until 2016. Onwards absolutely on GDPR roles. So, two projects and Bank X prior to my time in GDPR. So by the times of GDPR I help with implementations of GDPR. I do that for financial institutions such as Bank Y, Dutch insurers mostly and the Dutch Authority of financial markets quite recently. Those kind of clients. I used to work for a consultancy firm and since 2019 I work as a contractor, I help companies implementing GDPR

Question 2: "I would like to start, first of all with the trainings. Have you been participating or organizing sessions like trainings or seminars through organizations before the implementation of GDPR?"

Answer 2:" You mean before 2018? Before the official publish of the law. Yes"

Question 2a: "Can you elaborate a bit? This was driven internally by your organization or it was like a joint effort like from legal, compliance, IT for example?"

Answer 2a: "Usually I was an external so the company hired me or my firm, to actually give trainings or for awareness. So maybe compliance, legal or maybe HR were involved but limited. Really limited, because they hire externals like me with high costs so to cover like 90% of the whole. Planning for the location and staff was done by the company itself. The content of the training was provided by me also supported by internal people. And it's really good, depending on many different departments like HR, legal (not so much), compliance but also first line of business units. Your scope also includes insurers?"

Question 2b:" Yes and also if you spot any differences between the insurance companies. Were those sessions mandatory? Because what I am interested to know is where we stand at this moment. What usually happens is that all the organizations they have created a foundation. So for examples, new employees joining a company, they have to follow a GDPR training that is mandatory. But also do you think at this moment, three years after the release, is everyone up-to-date? Do we need continuously knowledge sessions for improvement?"

Answer 2b:" Many companies in transition are doing really good work. Training that were given at the beginning were forgotten most. There is strong demand, both in banks and insurers for more trainings, more detailed training. And I would say there is more demand than in 2017 or 2018."

Question 2c:" Why do you say that? Why do you think that is happening?"

Answer 2c:" Because people feel that training or awareness are very important parts for GDPR compliance. Initially it was legal much involved and there managers to understand more and more that in order to have a stable level of compliance, but personnel were more on the level that they work with data. There were trainings that were too generic in the past or focused on theory and maybe to a limited number of people. Now there is much more focus, more demands for trainings. We have financial business cases to get the training to HR people and then we focus on HR specific on GDPR."

Question 2d: "Have you faced, maybe not you because you are external, any resistance from people? Everyone seems to be easy to participate in those sessions? "

Answer 2d:" In operation with my client and some at higher level because they can enforce people. If it is not enforced by high level manager or by someone at senior level then training does not make much sense. I would say because people are not paying attention, they are not selling out, people don't take it seriously. I mean for many people it's not fun to participate in a training beforehand, I want to make it as at most as possible and I tried to be very practical, with a lot of games and fun stuff. Most people they don't come with the best compliment you can get. They say: it wasn't as bad as I thought. If anybody is only sitting there because the managers force them.

Question 2e: "Would you consider that maybe could have been done better and to raise awareness before those trainings so that they can capture the attention of the employees?"

Answer 2e: “Yes, definitely. So I would say a large portion of employees also have data experience, they think they know cleansing. Beforehand they think it’s not needed for the training for their cover. It’s the same with driving, there are many bad drivers but you and me we are part of the best drivers. We don’t cause traffic etc. That copies now from work, proving because they also try to listen better to employees for the type of training targets. Like less theoretical, more use cases. Practical appliances of GDPR and less talks. For example, I remember in 2016 everybody was focusing on fines. It’s discouraging in regards to the fines but you should really triggers them in their day-to-day work and then such training can help. It used to be like, we have a new regulation and people to get trained because there is a fine. It doesn’t seem very strange.”

Question 3:” In that sense, do you think at this moment that they are also investing on making a knowledge base in their organizations, like having work instructions and guidelines?”

Answer 3:” Yes almost every department does.”

Question 3a: “Because I can imagine, and this how it was perceived; that initially we have projects dedicated but people need to move more to the business as usual phase and then of course this guide from operational side that need to be in place. The necessary work instructions also for audit purposes.”

Answer 3a:” That is where the most companies, including the large ones, weren’t given enough attention and therefore I am busier than ever because I have little rework. They haven’t done it right in the first time so now their trying it for second time”

Question 4: “Topic of training part has been covered so moving on, have you been consulting on the way they are conducting the PIAs of DPIAs? Maybe you can elaborate a bit on how ,and if, it can be done differently between insurers and banks. Maybe also on which level are they doing. System level, data level. Most of the companies they are doing it on processes, they are trying to identify the processes but also on system so that they can register some inventory”

Answer 4: “I wouldn’t say that, it depends on the tool and all the people guiding the DPIAs. I wouldn’t say it’s different for insurers.

Question 5:” So, would you suggest or consulting your client to do it on system level and then dive into the data?”

Answer 5:” We generally advise clients to do whatever is required to launch a new system. And if the system contains personal data or sensitive data. But also you should do a DPIA whenever you encounter higher risk processing. Generally we invite clients to do it that way, because otherwise they should convert the DPIAs, escalated by the highest risk to be at the system. Every client has it in his backlog”

Question 5a: “Those DPIAs, are you doing them on a yearly basis? Or there have been any changes after moving in the time compared to how it was before.”

Answer 5a: “Systems are brushing things as we would like them to do it. Maybe on yearly or two years basis for the same system.”

Question 5b: “So you put a risk classification?”

Answer 5b: “Happy to cover one system once, because there is not enough manpower to the same system or process more than once. In theory we should do it every two or three years, based on the classification indeed, but in practice not possible.”

Question 6: “Would you do that on data level also? Like you have a system, what kind of data you have. By data modelling you see how data flows from system to system. So have data flowing between systems, you do PIAs on both systems, do you also think you should dive into the data fields themselves? E.g. this field is personal, this is transactional.”

Answer 6: “We have our data processes registered, and the requirements and then already we have some information. We go on the data as you said, it depends on what the client wants and how much activities he has. I want to see when we do a DPIA of the system how the system works and data elements of that. Because if someone writes a thing about a system, but if you see the system in your own eyes it gives you more insights on the PIA. So, I would say, especially high risk systems need more details to understand the system as much as possible. Especially as an outsider you don't know the system so high risk needs more attention."

Question 7: "Have you also been participating in projects dedicated to make an existing system GDPR proof? Make you can give some details on what kind of system it was, what kind of changes were there to make."

Answer 7: "There are many techniques to help mitigating the risks around personal data. One very difficult is to for standard stuff is let's say improving data handling and there are methods like anonymization, caching. I think I have advised several times."

Question 7a: "Anonymization and pseudonymization are called data sanitization methods."

Answer 7a: "For example we also have the OCIA classification so you check the authorizations, the implement Need to know principles. I think need to operate together I would say also for the ISO. They help you also with appropriate methods for mitigating the risks involved in the systems. So, I would say as a team effort you should classify together, have a different view. And then together work with the Privacy Officer to supervise the system. I would advise everyone following up the DPIA with relevant measurements because it is really important. Otherwise deeper ending will be met."

Question 8:" Are you also reworking on the DPIA process at this moment? I mean after three years that GDPR is live, do you feel the necessity that the DPIAs need to be reworked? Not per system, but more from methodology perspective"

Answer 8:" Some of my clients have their system DPIAs, with all the questionnaires and stuff, so we have updated and changed those. So many times the questions are not really understandable for the end user. They are written from a lawyer's point of view, and not from a user's point of view from technical point. We also change many times the process to run the DPIAs. We have to make sure that people want to do the work and it's easy and understandable for them as much as possible. And very often it is forgotten it's influencing GDPR. They are used in a way of working, focusing on themselves as professionals."

Question 9:" Are you aware of any projects or have participated in activities when it comes to the third parties – sharing data with third parties. What have you done there? Have you also been revising the process? Implementing also new tools for having guaranteed privacy and compliance requirements? "

Answer 9:"Yeah, although I must say it is not a very popular – it used to be on higher priority on early phase when creating the DPIAs and the processing agreements. But already for quite a few years, procurement does not like it so much and everyone was pretty much informed. And in my understanding, having third parties working up to the standards as required, it is not something that can be controlled adequately."

Question 10:" Based on your experience so far, would you say that you see a pattern or maturity levels? Do you think that big banks in the Netherlands are reaching the level that is adequate for the regulation requirements? Do you think that some have exceeded it? How would you evaluate the current status? And maybe what are the actions to be taken?"

Answer 10:" The large banks , they can have more data and export more data. That does apply to insurers to a lesser extent. I think what the big banks are currently do, Bank Z, Bank X and Bank Y, is insufficient. For insurers, due to their scale, their standing in society and the type of data they are holding, I would say it is less disappointing."

Question 10a:"Where do you think this insufficiency comes from? Is it lack of awareness? Underestimate the impact of the regulation compared to the old one? Culture? The higher management has not raised awareness maybe?"

Answer 10a:" All the big banks they have big problems, and they have to invest to solve them. But generally if they find it important they would pay the highest rates or hired more people to work on it. And then also make sure, because it’s important that everyone Top-Down complies. Prior to GDPR I worked in other regulations, the budgets for those were much higher than the ones for GDPR. Basically, the most important thing, is that they are investing on other priorities.

Question 10b;” Because in my research questions I am looking for like, GDPR is here for good, whether there can be twist. Everyone has to be GDPR compliant to avoid fines, to avoid reputational damage. So we try to find whether the basis and the principles of GDPR can have a more opportunistic view on things rather than only comply. “

Answer 10b: “Most companies seem to be biased. They don’t implement GDPR because they feel the principles are right. As a person I think the theory is quite important, sometimes difficult to understand. But the companies follow it as another obligation. And that is really a big mistake. For example 9 years ago in Bank X, they used to do things because the regulator was asking. More jumping priorities in another regulator was here. They never thought why don’t we stretch our legs so that we jump first. They are always reactive and that is more we follow what we have to do. Never think how we can be ahead, and that is something I am really disappointed and of course we have discussed it with some people and most of them, possibly because of the nature in the organizations to react to regulator and not to think why they are asking it, why don’t we understand what they will ask in the future etc. It is very difficult, also for consultancy firms to decide this kind of things.”

Question 11:”So, in a nutshell of what you just said, the companies have not reached the sufficient level of maturity, although moving from project phases to BAU and more integrated activities.”

Answer 11:” I would say none of the firms I worked for, have reached the maturity expected. There are always risks, it goes so slow. They keep taking it non serious and invest a little and every time they try to stop the flood for drowning. But they never think how we can prevent the flood from happening.”

Question 12: “Do you think that there is a wrong a perception that data for example are a matter of IT? The new law is about IT systems to restore, edit , delete data. So that the perception is that IT should be investing on those projects. What I see is different perspective from IT side. Now with technology we could make whatever we want but if you don’t have the necessary principles in place “

Answer 12:” I would say GDPR is less about legislation, less about IT. But it’s more about culture and people to the most of the companies I have worked. In that sense I support this statement above.”

Interviewee F

Question 1:” How have you been participating on trainings related to GDPR, before the implementation of the regulation?”

Answer 1:” Before the implementation, we actually had a specific group focusing on that, we had some classroom type of trainings about what is privacy and where does it interface with the processes of the bank. So, a general classroom training about privacy and certain aspects of that, like principles etc. from the old, pre-GDPR directory.”

Question 2:”All those trainings, were internally organized by the bank or you had also external specialists to participate?”

Answer 2:”No, we did have enough expertise in the bank to do it ourselves.”

Question 3: “So, from structural perspective, I can imagine, because we are dealing with regulations, legal might be one of the driving actors let’s say, for the learning sessions. Compliance also. Is that correct?”

Answer 3:”Correct. Myself I am from Compliance, I work closely together with our legal colleagues and certainly the privacy officers. “

Question 4: “Did you also have specialists participating from IT side, from data management or data controllers for example?”

Answer 4:” Sessions were mostly organized on demand, so we have done something like this for the security and marketing department. And also for the compliance colleagues as themselves, as a generic compliance office.”

Question 4a:” Did you notice during these sessions, that there were different perceptions that data is something related mainly to IT departments, as they are handling data, and for example people from compliance have a more theoretical or regulatory driven approach?”

Answer 4a:” I think there are different views on personal data. Marketing people feel they are using data of the bank, whereas it is not owned by the bank, it’s about the individuals and they appear more to take care of the data. Sometimes when I look at IT people, they see privacy pretty much in terms of security so more like confidential and not if the usage is allowed.”

Question 4b” Alright, so you would say in general, that we need more diverse workforce, in order to implement this kind of regulations?”

Answer 4b:”Absolutely, I think it’s multi-disciplinary issue that needs to be implemented combining all the necessary disciplines. Security is one of the aspects, yes, people from information should be involved, people from data management, legal, compliance, all parties have their own specialist knowledge, but also their own needs. Need to look at it holistically on how to implement.”

Question 5:” At this point that we stand today? Let’s say in the meantime between those sessions you are referring to until now, do you have regular re-trainings or sessions or ad-hoc learnings to keep the topic hot?”

Answer 5:” As part of the implementation of GDPR, we have introduced an e-learning for all staff, so basically every employee and newly hired should follow it and learn some sort of the basics. Next to that, we have a tool in the bank that actually people need to answer questions on various topics so privacy or compliance on broader sense, security and safety, and people need to answer questions on a regular basis so it’s an awareness tool to keep the information and the awareness high. And we have just finalized upgrading our e-learning to aim more on differentiating our e-learning. So depending on your role you go on different path because the previous one was more generic. So everybody had the same level of knowledge so we are trying to more specialize towards the role”

Question 5a:” So, indeed it seems that already all this period things about learning and improving the way of dealing with the regulations is still ongoing. Based on what you just said, I can imagine that for employees and new joiners are mandatory, but now it’s a bit customized on the role. Are all those mandatory?”

Answer 5a: “Yes, they are. Next to that we have some classroom trainings there are all e-learning based, so everyone can do it for himself. But there are also classroom for privacy contacts in the business or special training for senior management and the board for example, to keep everyone aware on how the privacy is important and what sort of issues and dilemmas can come up. “

Question 6: “Based on the outcome I have from previous interviews, initially people were more exploring what it is about the new regulation but as they have moved and processes have been revised and reintegrated after the implementation, they are coming with more tangible examples, and crucial questions during the sessions or incidents. Did you phase the same?”

Answer 6:” I think that is true. As awareness and knowledge level rises, people recognize more issues around the topic of privacy and therefore also things they have been doing for a long while they suddenly realize “ Wait, is that something I can do based on privacy? Or is it something we should stop doing? And that is one of the big advantages of training people and raising awareness.”

Question 7:” Do you also have some work instructions or manuals in place, available for the employees?”

Answer 7:” So, we have policy in place which is very high-level. And then we have a number of guidance in place that make the policy more tangible and describe what we have to do. And those have to be translated into work instructions by the department themselves. Because the departments are so many, we cannot do that centrally. But the policy describes the way to follow to translate them.”

Question 8: “Have you noticed any resistance from the employees to comply with the new rules? Because usually were used to old processes and most difficult is to change the attitude or the new way of working with an old system or even a new system. “

Answer 8:” Still I see that on some new systems for example, I see that from people that they have a very clear goal for example the information security department. They want to do fraud detection which fraud detection can skip some of the rules. Or Anti-Money Laundry detection and even for duty of care issues. It’s not a conflict but there is some tension between GDPR and their objectives. And those people are very convinced of what they have to do, and they see GDPR and ask all sort of questions and see that there is a reason why we are looking at it. There I see some resistance or we need to do more convincing compare to employees that are in contact with the clients- there are more happy to follow the rules.”

Question 9: “Moving on to my second aspect, is the data systems and the policies on them. There is effort needed to make them GDPR proof. I can imagine you have been also setting the policies, or called best practises or guidelines for conducting the PIAs? Can you elaborate on how you do that? On process level or per system or do you dive into the data, data attributes themselves. And also a bit about the policy, how often do you have to revise it? Or when you have a new request for a field to be added? ”

Answer 9:” We have two areas where we do privacy impact assessments and the assessment itself it’s a short questionnaire which PIA triage just to determine a data protection impact assessment needs to take place. One area is around changes, so if there is a change on the process or a system or on a product even, there is a change risk assessment process within the bank and as part of that change assessment process also a PIA triage needs to be filled-in. And depending on the outcome a full data protecting impact assessment is required or the privacy aspect will be taken on board on the data change risk assessment. That can be on a system level or process level or even on new product or the new way of organizational changes. The second one is the process level, if you look at GDPR we need to have an inventory with all the personal data processing so need to have in on process level too. All entrances into our register also go through a sort of a PIA triage in order to establish the level of inheriting risk. And if it is a high level risk then we ask the owner of process to do a PIA. That’s a long process, takes long time in a big organization like our bank is, there are a lot of processes. “

Question 10: “Did you also have to revise the record keeping and retention policy around your data?”

Answer 10:” Not so much revised the policy but the implementation of the retention part itself. The policy has been updated to have a clear ground on the retention policy, see it from legal obligation or from the legitimate interest of the bank, in the end turns out both can be valid. We have retention policy and retention schedule but not all systems especially legacy systems, can go to deletion on an automated way. There are still some systems that will disappear at some point and they cannot simply adapt to make it fully compliant. So we really focus on new systems there we can invest on build that functionality. ”

Question 11: “Do you use concepts like data lake within the organization?”

Answer 11:” There are some data lakes, also legacy, we see now that data management go now on new approach, they have controls, interface where the data users and data owners can actually agree on the use of data. And as part of that, on some cases a data lake will be created, because the data is used very often, but in other cases every use will go through an interface and go right strictly to the system, the source.”

Question 11a:”Because there is some sort of contradiction, data lakes were about to provide access more horizontally in an organization, and in the same time we have GDPR which is more restricting the access to the data. So you say you have a control interface and for that interface do you use methods of sanitization like anonymization or pseudonymization of data?”

Answer 11a:”No, the interface is more about controlling who has access to what data. It’s not complete yet, not all data goes to the interface, and also the functionality of the interface is being improved and enhanced that will take a least a year. There are things like segregation, and database that on table rows and columns can be done and getting filled only by the records that you actually need. But that is still work in progress. There is still the idea to build a control who is using data for what purpose and there is a data check if is that allowed, like applying purpose implementation principle. Then data minimization is now being built on row and column level. And the data lakes, for as far as they exist, actually have to do an assessment on each use of the data lake.”

Question 12:”So sticking to the rules of GDPR, of the purposes of using the data and the expected timeframe. Coming now to external providers, usually banks have third parties handling data, or now with all the transactions and the methods of payment, has GDPR affected the transfer of data to external providers?”

Answer 12:”We use a lot of service providers ourselves, as third parties, and those are most of the times processors on behalf of the bank. For those we have clarified whether we have correct data processing agreements and if the data protection processes are in place. That is where we use third parties. Sometimes, we use third parties who are themselves controllers, for example a credit rate rating agency which check if our clients have certain debts. Those are controllers themselves, so we have setup the right contracts to do that. In some cases we deliver our data to third parties and those we check if they request they do are compliant under the legal obligation. We look to the legitimate ground of transferring of the data.”

Question 12a:” So, there was need to revise the DPAs (Data Privacy Agreements)?”

Answer 12a:” So we looked at it when GDPR was implemented and now we have to look at it as a continuous process. Check what need to be renewed etc.”

Question 13:” Is it you a Data Privacy officer that you have on yearly basis to revise/review the policy and the processes?”

Answer 13:” We have two things, where can use our own DPAs or our own contracts. In Microsoft for example, you have to use their terms and their contracts. But in smaller third parties we use our contracts and we do a check whether the right content is in the local contract. We do default contracts or local. Then we have a control we are monitoring and testing on a subset of the contracts to see if they are correct in terms of the DPA and things required. That is done on a half year circle, not for all contracts but for a selection.”

Question 14:” Last section of GDPR, where do you think you stand at this moment? Do you agree that most of the projects and the activities related to GDPR are moving more to the BAU, integrated in the daily operations of the organization? Or you see that there a lot of things to be improved?”

Answer 14:” I think we had the GDPR program after 2018 that it came into effect. After that it took another year to finalize the issues. And actually there are a few that has been decided like legacy systems issues decided not to go to fix but wait till they will be replaced. That is certainly BAU now and the expectation of both the supervisor and the general public is still rising. Even though is BAU, I think, we probably need to bring more attention again in the coming period to reach next level of maturity in that sense.”

Question 15:”We highlighted before, that employees are getting more and more aware or cautious around the topic. I would to switch the topic now, have you also worked for PSD2?”

Answer 15:” I have been involved yes.”

Question 16:” Sometimes there is lot of discussions or papers, whether GDPR and PSD2 are going hand by hand, especially when it comes to the client consent mechanism. But also based on my research phase and the interviews, we see that GDPR is giving really clear guideline and principles, also around the consent. And PSD2 is lacking behind on specifying what client consent is. Do you agree?”

Answer 16:” Yes I agree, there is a difference between the two. This is concerning because we have to manage them both at the same time.”

Question 17:" How much have you been involved in trainings about PSD2 readiness before it was implemented?"

Answer 17:" For PSD2 it doesn't require a lot of training for general staff. Because PSD2 to a larger extent is within the systems itself. Our bank decided to have an API approach which is the systems of the third party providers and interfacing directly with the APIs of the bank. So actually there is not many staff that need to be trained in any detail. Except only if people call the contact centre and the employees there need to understand when people start asking questions about PSD2 and what that means. So we have introduced some script for that to answer the most likely questions of our customers."

Question 17a:" And do you need them to be continuously trained?"

Answer 17a:" No, not so much. Because as I said for PSD2 there are questions that pop-up and those might need to be updated, but that is not necessarily require additional training."

Question 18:"In regards to the readiness and the maturity that the bank stands now, do you think the expected levels of maturity have been achieved?"

Answer 18:" I think our bank is the only one managed to have the API in place before the deadline, September two years ago. But since then, let's say there have been new views on the way it should be done. Whether a single customer authentication should be enough or we can do double to authenticate the customer then to be able to authorize payments. So, in the end we had to adapt the whole system again and that actually meant that could offer another way, next to the API, to PSD2 projection."

Question 18a:" Last June the EBA has published the revised guidelines. Are you referring to this?"

Answer 18a:"Yes indeed, that had an impact on our implementation and then we have to change that implementation and allowed us a different path for TPPs to access account data"

Question 18b:" Because there were major incidents around the reporting and it urged them to publish the revised guidelines. That is a finding by itself in my research process."

Answer 18b:" That is a strange play. There should be also a certain interest that they want to push through but yes. So, in terms of maturity, I think we are still finalizing the new implementation,that really impacted the core of what we thought it should be implemented. Also keeping an eye on the security for our clients. But EBA was very clear that part is not up to the banks but up to the TPPs' responsibility and therefore we should this step back. PSD2 as such is well embedded in the organization, there is team that deals with it specifically, and there is a product owner so really one of the normal processes now."

Question 19:"Is there any further actions or steps, you said it stands as expected, so I guess of course everything is continuous work."

Answer 19:" We have the Dutch Banking Association that received the letter from the Data Protection Authority on the data minimization issue on PSD2. That came as a surprise to the banks because there was nothing related to it in the PSD2, certainly not from the Dutch Central Bank."

Question 19a:"When was that?"

Answer 19a:" I think half a year ago. We received a letter on we shouldn't give access to TPPs on all account data but only to the data required to deliver their service. That again from bank's point of view is a new requirement which requires again back to the way we implemented and see how can accommodate that. And the way the bank sees it and the way I read it, we have to limit the data to specific fields required by the TPP and then allow the transactions based on the fields required."

Interviewee G

Question 1:" What do you think was the impact of GDPR compared to its predecessor regulation? Do you find major differences so that the impact of new law was big?"

Answer 1:"Yes, the impact of GDPR is quite substantial, although the basic rules are not that different than before, the level of organizational demands from GDPR makes it all and all quite impactful. Because you have to lay down all your processes etc. and of course also the attention in society for GDPR also makes it automatically with heavy impact."

Question 2:"Now we stand more than 3 years after the implementation, have you back then, participated in training sessions ,e-learnings or mandatory courses among the organization?"

Answer 2:"I have done the e-learnings, but everyone has to do them."

Question 3:" Do you think that now, that we have moved in time, I understand that the beginning it was more project phase, now is more integrated on the business as usual. Do you think that the employees need to be constantly trained on the topic? Do you see differences on the awareness than before?"

Answer 3:"I believe that in the sense of GDPR people are more aware of privacy. And more aware with the fact that you cannot do whatever you want with personal data without checking it first. Not sure whether the e-learnings that everyone has to do are decisive or whether it's just a common knowledge for GDPR."

Question 3a:" My questions is more about, shall the organization invest more on continuous learning? Do they build libraries with work instructions and guidelines for the employees? One thing I know it's mandatory for all new joiners to follow the e-learnings, but when it comes to build a foundation around the topic or working on business cases now they are more experienced on what GDPR requires."

Answer 3a:" I do not know what kind of training product owners or IT people are getting. As a lawyer I am aware of the guidelines published by EBA and the Dutch Authority so therefore I am always a bit hesitant with letting people do their own judgements because of course need to take into account the data rules of the Data Protection Authority. So, I think a basic constant level of training helps, especially for awareness purposes. I don't think is efficient to train all the employees to a level that they can do their own assessments."

Question 4:"Could you tell me about your role in regards of GDPR? Were you part of a specific project? Did you contribute on the PIAs?"

Answer 4:" At the time GDPR was implemented I was part of a GDPR project (at that time I was advising primarily on the PSD2). At the moment, I am advising on GDPR topics such as should an assessment be done, what legal basis can be used. Those kind of questions.

Question 4a:" So, is it more on the data side or processes? Maybe on contracts?"

Answer 4a: " My role is to advise on the usage of data by Bank X itself."

Question 5: "Did you also participate on making systems complaint to the new law?"

Answer 5:"No, not for GDPR. More on the PSD2 side."

Question 6:" When it comes to the PIAs, revision of the questionnaires and align with the way of working in Bank X, do you participate in this kind of processes?"

Answer 6:" If someone has a question on the way of working, I can advise on it but it's like in a special audit department."

Question 7:"One last question for GDPR, do you think that Bank X is reaching the adequate level of compliance? Now 3,5 years after GDPR going live? Any points for improvement? How do you see the maturity levels?"

Answer 7:" I think the banking sector is in control when it comes to GDPR in general, not by product specifically. It would be delusion to say that everything is perfect. Not going into further detail, sorry."

Question 8:” I guess there is always field for improvement. At the beginning was more like, if you don’t comply there is reputational damage, have to pay some fines, so the organizations felt the obligation to comply because of these risks. Do you see the opportunistic side of this? Like privacy by design and all published details on guidelines and how to do your assessments and how. Do you think that now they realize and can twist it to how we can benefit and not only the obligation to do that?”

Answer 8: “Of course, can depend on who you are asking. My view is complying with GDPR has more advantages than only not getting a fine. That is how usually lawyers see it, the advantages of complying.”

Question 9:” Finding people for PSD2 was far more difficult than finding candidates for GDPR, I think I will use the rest of our time to discuss for PSD2. So, the questions would be pretty much on the same pattern. Have you been participating in learning sessions for PSD2? Sessions organized by Bank X or by externals? Because the score is not as big as GDPR, so how it was done?”

Answer 9:” I believe PSD2 is much more a specialist project, because we have to open up our systems to other banks and therefore it’s especially important that those banks can talk to each other via APIs etc. So, I can’t remember any broad training on PSD2 as opposed to GDPR where everyone had to do all kinds of e-learnings.”

Question 10:” Do you also see the necessity, let’s say, or the need that since it’s more specialized to specific departments, especially when we have to do with payments and IT on the APIs, do those people get yearly trainings or update of knowledge or it’s like one-off seminars to prepare them for PSD2?”

Answer 10:” it’s more that you are on exchange of knowledge, between what the regulator saying is and how the Dutch regulator is implementing PSD2. It’s more like an exchange of views from multiple sides of the bank.”

Question 11:” Are you aware of having some sort of library with work instructions or with business cases, that people can always refer to?”

Answer 11:” No, I don’t believe we have such a diverse library.”

Question 12:” I can understand that for this kind of regulations, we should bring different people from multiple departments in the bank at the same table. Was it mainly from legal, IT and departments dealing with transactions? How would you say it was the combination of expertise?”

Answer 12:” Usually we have a strong business representative, because he/she is responsible for complying. Getting advice from legal department but also has to work together with IT people.”

Question 13:” You mentioned the APIs, really common to be used for PSD2 purposes, were there new APIs used or there were already in place and need to be extended/adjusted to communicate with other organizations?”

Answer 13:” I am not sure whether there were old, there was already some data exchange before PSD2 existed but to be honest I don’t know what technique was used for that data exchange. Whether it was APIs or some other.”

Question 14:”When it comes to the third parties, because for payments we do have them involved. Do you have data privacy agreements? Have been revised for PSD2?”

Answer 14:” No, it is forbidden to make data privacy agreements obliged to exchange data. So, third parties have the right to receive data from Bank X without an agreement being obliged by Bank X.”

Question 15:” How do you achieve the consent from the customer through the contract? And then the customer trusts the bank will use the data for specific reasons and purposes?”

Answer 15:” PSD2 is quite difficult from that perspective. Perhaps an industry letter can be sent to you and you have all kinds of permissions and agreements a client has to give to its TTP and to its AISP. The regulator made it quite clear that it’s first and foremost when it comes to PSD2 data exchange, the AISP has to make sure he has the consent of the customer.”

Question 16:” Last June we had the revised guidelines published by the EBA. What was firstly published was not compliant with the technical requirements. Then the Dutch banks united reacted and then there were the revised guidelines published.”

Answer 16: “You mean the guidelines on the interplay between PSD and GDPR?”

Question 16a:” No, I refer to the ones for PSD2 only”

Answer 16a:” I believe in June or July in 2020 the guidelines on the interplay between PSD2 and GDPR were published. But in December the same year revised version was published and the first one version was without industry comments and in the second one industry comments were taken into account.”

Question 16b:” That is the one I was referring to. How did that impact Bank X and the departments working on it?”

Answer 16b: “It’s quite difficult, because it’s sensitive information to discuss the Bank X situation but therefore the industry letter must useful because it’s public information. In the industry letter some of the main issues are discussed.”

Question 16c:” My question was more, did you have to stop a way of working and immediately change? Did it impact you that way?”

Answer 16c:” I’m afraid I cannot say.”

Question 17:” What do you think about the levels that Bank X is complying with PSD2? Do you face major issues? Do you think is in control as for GDPR?”

Answer 17:” Nothing is perfect but I am also going to give an answer on the banking sector in general. I believe that PSD2 has had the attention it should. Of course the publishing on new fuse makes it necessary to keep following the guidelines.”

Question 18: “Question for both regulations, maybe more relevant for GDPR. Did you sense that people were more reluctant at the beginning with the GDPR topic. When we have to move from project phase to BAU and integrate some activities in the everyday work, people being more relaxed but now getting more aware because they see things in practice? How would you characterize the people factor?”

Answer 18:” It is accepted that when you are a bank in 2022, all kinds of regulations apply to you and of course if someone has to do a lot of work because a regulation changes, they are not perhaps jumping up and down his chair with joy, but it’s part of the job.”

Question 19:” I guess for PSD2 it was at lesser extent cause the impact was not among the whole organization.”

Answer 19:” PSD2 is not small it shouldn’t be underestimated but it’s not as large as GDPR is.”

Question 20:” Did you know if they have been moving in cloud based solutions?”

Answer 20:” No, not in my scope”

Interviewee H

Question 1:” For GDPR, have you been involved in organizing trainings and also participate during the sessions?”

Answer 1:” I have not been involved in organizing. I have been trained in GDPR but was not a trainer or something like that”

Question 2:”At the stage that we are now, e-learnings are mandatory in each company. Every new joiner has to follow. What I understood, and you can tell me whether you agree or disagree, like people at the beginning they were more on the theory side, more about raising awareness about GDPR and what is coming. But now, three years after going live, do you see the necessity to understand more about GDPR? Do you have like specific incidents that might have been treated differently?”

Answer 2:” No incidents really. What I think is that the level of what personal information is on GDPR is so extremely low that constant awareness on what actually constitutes these involved data is required. So, for example an email address is personal data. People should be aware of it and constantly be reminded of it.”

Question 3:”I’m trying to understand if this continuous knowledge sessions, I heard from some consultants that people are reacting differently today because they have seen business cases, they see things in practice and at the beginning was more about theory. So, awareness is always there, and people are coming with tangible examples.”

Answer 3:” I am mainly working in the wholesale environment where by this is less of an issue when you are working with retail clients or real persons instead companies. I think in the wholesale environment there are sufficient ways of working around it.”

Question 4:” Have you been aware of what a PIA is , or DPIA? It was imposed by the regulators that the companies have to conduct.”

Answer 4:” I noticed it happens but I am not involved.”

Question 5:” Any contribution to a project or implement a new system that is going to handle personal data? Or making an existing system GDPR proof?”

Answer 5:” No, but I have been involved in projects whereby we must ensure that the personal protection of our employees is being protected. For a different company I did the negotiations on standard documentation and always GDPR was one of the elements which we ensured that was fully documented.”

Question 6:”Did you also have to revise like authentication, access rights and who has access to the system or encrypted some information?”

Answer 6:”No, that’s really on the systems and I was more working on for a party which has multiple bank services. The documentation, the general conditions that needed to sign, needed to be GDPR compliant, ensuring the rights of the banks to ask for details on a person. But no system wise implementation.”

Question 7:” Do you think, when it comes to the people, that there is a perception because data is about systems, that the GDPR topic about personal data is more an IT matter so it has not been given much attention as it should from other sides of the business?”

Answer 7:” Well, working as legal counsel I can say that definitely it has got a lot of attention, also outside of the system areas. This is not something I directly recognize to be honest. But I am working in the compliance part so that’s less than when you may be working on a business environment that you should handle new propositions. That’s different than working in a compliance, legal or risk department.”

Question 8:” Do you think that today, that we are more than three years live with GDPR, that things have moved from project base to BAU? Do you think that the actions the banks have taken are adequate to be complaint to the regulator? Do you think they are not mature enough?”

Answer 8:" To be honest I don't have that insight."

Question 9:" Do you agree with the legal baseline of the consent in GDPR?

Answer 9:" I think there are tremendous difficulties in fully implementing it. For example, the lack of obligation from the employees that is not possible to ask them for consent. If you look into the consent requirements, which you have online as a person, you don't really have real options available. And even maybe you explicitly need to tick box, which very often is not the case, that is being rounded off by a lot of instances. You don't have an option if you want to buy or purchase certain goods. So, it doesn't really fully help, at least there are some checks and balances, which is an improvement from which there was before."

Question 10:" Do you see some correlation between the consent topic in PSD2 and GDPR?"

Answer 10: " Cannot answer. I think PSD2 it's a bit, generally speaking, bank regulated. So they are more inclined and used to asking for permission and checking several boxes etc. So what needs to be asked explicitly, they ask it explicitly. While in a lot of more consumer based industries people just want to sell, and they are less inclined to have these questionnaires. So, from that perspective the regulated environment is in front in the compliance."

Question 11:" Have also been trained for PSD2?"

Answer 11:" No, not really."

Question 12:" Any comment about the revised guidelines published for PSD2 and the APIs? Because the impact of awareness was at a lesser extent compared to GDPR."

Answer 12:" If you look how some banks have implemented it, it's hardly accessible there, so in theory maybe they have an accessible API but there are still so many steps to be taken and some IT solutions needed. That is not like you can easily access every bank, everywhere. Especially from people working with banks in Spain, their APIs don't work if a third party wants to make use of it. I am really up to date with the revised guidelines, but I know before that, that it was almost impossible."

Interviewee I and J

The last interview session was held with two interviewees (I &J), therefore the transcription was done for both at the same time as well as the decoding of the interview.

Question 1 to Interviewee J:"Before the implementation, have you been involved in organizing training sessions? Do you have some sort of e-learnings that are mandatory among the organization?"

Answer J:" So, if I was involved, well yes. I think we have set up learnings internally for the colleagues who are involved. I think initially it was really meant for those who are going to deliver the services,that are so closely involved in the project organization, to explain what PSD2 is about. Normally I always explain, what it takes for bankers. It's really difficult where we have one to one relationship with our customers and suddenly there is a third party. For bankers it's an awkward feeling, there should be two in this relationship. And I think that is where I really see the difference in mindset within the banks. It was really different, because we were used to have that monopoly on the relationship with our customers. Of course we have competitors, but the competitors sell their own products via their own channels directly to our customers. And I think that concept of the third party in between, where always the customer remains our customer, but there a third party also playing a role. That was the most pivotal element we always have to explain towards our customers. That was the key part of the learnings for those who are part of the delivery organization projects and also had to set up the proposition. Later on in the process we also set up quite some annual e-learnings for customer phased employees, so for those who are in the contact center or those who are in the branches. In height sight, I don't think that as we see the take up of PSD2 is now limited, even stuck a bit. I think we did an overkill of explaining the concept of PSD2 towards our customer phasing employees, where they did not get so many questions. We still had a spiker, I think at the beginning a lot of people were curious about PSD2 but later in the process the after curiosity was over. Imagine when the customers see their real added value and the value was limited, and therefore the wish he did decline in the use itself all the services, across the market. So, you learn it by project organization, helpful is explicitly to define the role there with the three parties and what is the difference between user experience and an API and how data will flow from left to right and the third party and later on, via learnings towards our customer phasing employees. After inside it didn't cost the limited number of questions."

Question 1 to Interviewee I:" Anything to add from your side?"

Answer 1:" No, that period I was not involved in the program."

Question 2: "So, I can understand that at the beginning it was more about raising awareness about what is coming. Now that we stand almost four years after, do you see that these sessions should be planned continuously? Or need to be revised? Maybe change the way of conducting those trainings like now we have more issues to deal with or more business cases? Did you recognize this kind of changes?"

Answer 2 – Interviewee I:" As per Interviewee J was saying, if you are looking at the usage of PSD2, it's quite limited at this moment. Big drop off numbers after the new gambling law in the Netherlands. So, the benefit of having extra e-learnings at this moment, I don't see it at this moment."

Answer 2 – Interviewee J:"I think, what I observe and I have now and then discussion on PSD2, I don't think that the PSD2 services as defined currently that they will grow. I think they are kept at what the possibilities are given, how the market acts and how the market evolves. I think is really hard for a third party to get into business cases based on PSD2 services. So I don't think that PSD2 on its own will evolve too much richer services for TPPs. But I think there is still the latest interest for mainly organization to use PSD2 live services and exchange automatically information at a more standardized way. It would be more interested in the future on how businesses like software companies, on how they can exchange information, on behalf of our business customers. I see there a big demand and growing usage in the future and I think PSD2 starts with the consumer market. I think is the moment we start interacting on an ecosystem for legal entities. Then we have to initiate the learnings, I think for the consumer market PSD2 is close to that."

Answer 2 – Interviewee I:" My answer on the continuous training was no, and Interviewee's J was maybe but not on the consumer side but more on the business side."

Question 3 – Interviewee J:" I heard that you mentioned that you were part of the EBA working group? Last July, we had the revised guidelines published that brought a change to the approaches towards PSD2. I guess that have been impacted the way of working also in your bank? How did you experience that?"

Answer 3 – Interviewee J:"I am not currently involved in the EBA working group, I have handed over my position two years ago."

Answer 3 – Interviewee I:" There were the new guidelines somewhere in the middle of last year and we had to make some changes and then do some additional work. And we did what was requested and it was a little bit annoying maybe."

Question 3a:" So you had to adjust to a new way of working. And when it comes to the third parties, did you also have to revise some of data delivery agreements?"

Answer 3a – Interviewee J:" We don't data agreements with TPPs, those are all part of the log and they come any certificate to open up our doors. I don't think we altered our APIs specifications based on that. I think it's the functional scope where we had to make some changes, but not on the technical interface. I know that we have for the technical interface but we don't have a data usage agreement that GDPR calls nicely. We don't have with TPPs, it's binded by law."

Answer 3a – Interviewee I:" No, no changes."

Question 4:” Do you see, because the legal basis for GDPR is the client consent and sometimes we see approaches that PSD2 and GDPR can go hand by hand because of the consent mechanism. Do you agree with this argument?”

Answer 4 – Interviewee J:” That was one of the biggest arguments in the industry at that moment, to whom to give customer consent of the usage of the data. Is it the customer who says to the third party, you can use my data for these and these elements or is it the consent to the bank to say “dear bank, please provide me this kind of data towards TPPs. We always state there are two consents: One, how can the data be used by third party. Secondly the consent towards the bank to provide data to the third party. Those are two different types of consent and from market practice TPP was argued that there should be one consent towards the TPP, that you can use the data according to it. Give me consent towards the TPP and there should not be any consent towards the bank. I think that was always a difficult discussion we always argued that there are two different types of consent and the GDPR consent that you use this data for those purposes. I know we always agreed that that consent is not with us and we are not going to check how the TPP is using the data of our customers. That is something between the TPP and the customer.”

Answer 4 – Interviewee I:”You know, this was not so clear for the client. Sometimes they call the bank, sometimes they call the third party. Also the third party said call your bank and we said OK but this is an issue between you and the third party, which was also difficult to explain to the client and to whom he gave this consent.”

Question 5:” Except from the APIs, did you use any other IT solution during the implementation of PSD2? Like moving to cloud-based solutions for example?”

Answer 5 – Interviewee J:”So what we did within Bank Z, we use the opportunity of PSD2 to centralize the services across Europe. In Bank Z, at that moment we sold two branches, we are active in 11 countries for retail and 17 countries offering banking services, we said we are going to offer to the market which means that we have to centralize quite some services and we have to connect also those central APIs. Internally towards the local entities, we used not so much to move to the cloud, we still feel recently things are changing with new regulations. At that moment, public cloud solution like Amazon and Google are not an option. From regulatory perspective they said that services and data, especially from systematically important banks like Bank Z, cannot be in the cloud. So we were really hesitant to move things to the cloud. So, in our internal data centers, and there we had quite some discussion on how we are going to, because to route the traffic from external X Bakker coming in our system says: hey I am another Bakker and I want to get my data towards a third party. We have to know OK X Bakker is a customer of one of our local entities, because X Bakker is not a customer of Bank Z Group but can be a customer of Bank Z Netherlands or Luxembourg whatsoever. Come and deal with quite some discussion, can you centralize some data from our customers without the customer knows or even need to know it. Then we can centralize partly the data. I don’t think they will be, there were discussions since June. So it was not much from the cloud perspective/ usage, it was more on where do you store the data, can you store the data of your customers even within one legal organization, Bank Z Group, which is publicly listed in Amsterdam. Can you copy this local data into a central system? We mainly had discussions with Germany and Luxembourg, Poland where local regulators. We are not talking to move data of their citizens into the Netherlands because there is our central data warehouse. So, that was more discussion from the GDPR perspective, can you transfer data to another country within the Bank Z organization, that was more of a discussion of moving towards cloud.”

Question 5a:” Alright, any other solution that might have followed or the way you are doing the data management operational part?”

Answer 5a – Interviewee J:” No. I think what we did, we store centrally few elements of the customer to route the traffic. For the rest it was more or less, we used the central system routing mechanism to go to the local entities. That’s all API based. Of course not only API based, there is a UX flow, a user interface where you as customer can select which accounts you want to give access towards TPPs. So, there’s a small element of UX and the rest deep based on the APIs. Not sure if that answers your question or that you are looking for something.”

Question 5b:” No, it does, because we are looking especially for PSD2, the main technology aspect is around the APIs and I was looking for GDPR for example, if there were more activities to make the systems more GDPR proof, give access to the right people. Some data sanitization methods like anonymization. But for PSD2 I understand the main thing is APIs.”

Answer 5b – Interviewee J:” We had one discussion and that was about the interface towards TPPs, which we said that we won’t have to redirect it via mechanism and then with the API you can exchange the data. The TPPs are very keen on using the screen scraping as a method which we were against. I’m still. Because with the screen scraping as a customer you don’t know which data is being screen scraped so it lowers our security measures because customers are getting used to exchange password information. So it’s a security thing but not for today’s discussion. From GDPR perspective, you cannot really prove towards the customer which data will be exchanged with the TPP. And so from a data minimization effort the whole discussion with the TPPs was, what is the data needed for the services described in PSD2. So we said for example, for AS we only need transactional data and balance data that’s it. From the TPP they said we also need to know which products you have and we need to have the dates from other products, we need also to have the home address. There was a discussion on what is the data minimum set required for the services described in PSD2.”

Answer 5b – Interviewee I:”That struggle is still going on there. The TPPs are asking for more and more data and we are saying no. Also I think the AP, the Dutch authority, is asking for data minimization.”

Question 5c:” Anything from your side Interviewee I, maybe to add?”

Answer 5c – Interviewee I:”No, as it has been said, we are mainly using APIs and lot of other things in the central database are already in place. So not new fixings we added to the IT landscape.”

Question 6:” How would you say that Bank Z stands at this moment, in terms of maturity on the compliance level? Is it adequate? In control? Exceeding expectations maybe?”

Answer 6 – Interviewee I:” I would say for the Netherlands we are fully in control looking at the PSD2 law. But is it satisfactory? We spent a lot of money and the usage is not so high. So yes, I think we have in place what we should have in place and things are working. We had some complaints at the beginning and some troubles, we solved them. I think we are quite great at this moment. Do you agree Interviewee J?”

Answer 6 – Interviewee J:” I fully agree. Strange if I would say were not adequate for PSD2. I think I would do exactly what was envisioned on PSD2 written. I think we actually live up to the momentum of PSD2. The only discussion still, there is no initial setup. There was a thought that there wasn’t viable business model based on the services described on PSD2. I think history turned out there is no viable business model that can be created on PSD2 terms only. So what we now see it that those TPPs, invested a lot of money. They said we won’t have a viable business model so we are trying to stretch PSD2 services to the max to get a viable business model. But I think that is a different discussion and that’s why we should be at the competition authorities saying fight with data privacy authorities. The data privacy authorities go back to the law and say yes they deliver according to the law. But the competition authority decides we want to create a market so we want to extend these services. I think now this is the tension between those two. So, I think yes we live up towards what is written at that moment. Do we enable stretch market? I don’t think so. But that is not up to us, this is because the law has been written with a certain mindset 10 years ago.”

Question 7:” One of the major principles of the regulation is to enable healthy competition across market and also encourage the banking organizations for more innovative solutions. Did you see that? Or it was more follow the trend when it comes to innovation?”

Answer 7 – Interviewee I:” Personally I don’t see any benefits from it. We did what we had to do and internally it’s a good exercise and we had some benefits from it, but for the market it was not. It’s a must, we have to do it, we spend a lot of money on it but benefits are not that big.”

Answer 7 – Interviewee J:” I slightly disagree. The reason is from perspective. From Dutch perspective if you see banking apps from the major banks Bank Y, Bank X, Bank Z they are quite advanced. They are not at the top edge of the market like they are fully integrated, like a chat app, like everyone envisions has the best in class for financials. But for the Dutch citizens are ok. Also if you look at the cost of the banking is relatively low in the Netherlands. Also from doing payments, sending money within the Netherlands of abroad. I think there are decently priced. So from Dutch perspective it was an add-on service without getting the benefits. But if you see it across Europe, some countries setting banking fees for just holding up an account, it's twenty times higher than the Dutch with poor services. I think there is a lot to gain so from a European perspective, I think what we have seen the last years, the fear of banks to lose the customer interaction, make that all banks had to increase in a digital proposition. That is what we have seen the last years in Europe that the digital propositions and a lot of markets that were underdeveloped, made a few steps, not all there yet, but made steps towards a better digital propositions towards customers. I don't think that we see a drop in fee increases but that's mainly because of the dropping the interest margin has to be made up by fees. I think that were the market circumstances which prohibited that. We see our drop of fees so that's the change. In the Netherlands, a little bit spoiled by withdrawal fees, recently decent propositions. I think in other markets in Europe they have seen a change in the market."

Question 8:" Switching to GDPR, have sensed different approaches. GDPR caught major attention from the society. There were also mandatory trainings for new joiners in each company and different kind of awareness raised. Have you been participating in organizing those sessions or seminars? Also before the implementation? But also moving towards the present?"

Answer 8 – Interviewee I:" I have not been involved in organizing. I was a victim of doing the e-learnings myself."

Answer 8 – Interviewee J:" I think I have a quite different perspective for GDPR. Interviewee I sees another obligation in the bank and that's why you say I was victim. I had to GDPR well where is not really affecting my daily work. I don't think that is what we have seen. A lot in the bank that people had to do all kind of mandatory GDPR training, while the benefit or the direct impact on their daily jobs were so limited. And to get there we did an overkill of trainings. For myself, I am a data owner, I have a few also data stewards in my area now which are responsible for checking on how we act with our data. So, I did same the trainings as Interviewee I as a bank employee but I did even a few more as data owner. I am not involved in the setup of trainings because there were centrally setup by the Chief Data Officer and the organization of the CDI. On my day-to-day business I had to free up resources to become a data stewards. Data steward is an official role within the organization, for which we can do a formal training, which can be formally appointed by the Data Council. So GDPR is affecting my job every day."

Answer 8 – Interviewee I:" I recognize what Interviewee J is saying, but he is looking it from a totally different perspective than I am."

Question 8a:" Do you see the need of a continuous knowledge sessions about GDPR, especially for the teams that you just described?"

Answer 8a – Interviewee J:" Yeah, because I think we are still in the interpretation of what the extent of GDPR is and how far you have to go. How are you going to monitor data but to ensure that you are in control of the usage of the data internally but also externally. In many cases as a data owner, I am responsible and accountable for certain data elements. For example, the name. But name is being used in many processes across the bank. Informally as a data owner, I am responsible that in each and every process, the name attribute is being used in a proper way and that if we display it towards customer or exchange it with the regulator, that all those things are pledged. Which of course I cannot do, let's be very honest, on the governance framework we are still evolving on how we are going to do it. We already see some tension on how are you going to setup this framework. Are you going to do it from a usage perspective? There is a data extract being sent to the Central Bank on daily basis. How are you in control of the extract? The data is always the same. You can have the same extract with crime investigation units. And there you see the tension of where do you have the checks and balances in place and to ensure the data is accurately in use, is complete. The data dimensions how you are going to assure. I think that is still where we have to evolve as an organization because it is easy to be overburdened with new policies which does not make it secure, but take a few boxes of GDPR then get this.”

Question 9:” Have you been also involved in the PIAs or DPIAs?”

Answer 9 – Interviewee J:” Formally yes, I signed those. I have 20 squads that I am responsible in my area. Each and every squad we make agreements that they will do the PIAs.”

Question 9a:” Do you do the PIAs on system, process or data level?”

Answer 9a – Interviewee J:” It really depends. We aim to do it at process level. How do you get it in daytime? In many cases at the process using a similar system and the data is same. I am the data owner so the teams they do not care about the data owner. They do their process and it all comes back to the data. I have to sign the PIA.”

Question 9a: “It is the traditional questionnaire that you have to fill in right?”

Answer 9a - Interviewee J:” Yes. We do that with the privacy policy department of Bank Z.”

Question 9b:” So you do that in the first place, let’s say like three years ago. Now do you feel the need to revise those PIAs? Have you also adjusted any processes based on that?”

Answer 9b- Interviewee J:” No, I don’t think so. You asked a few questions, do we have to revise, yes. Every time we do a process change we are looking when it works with the API. But do we have to change the process because of the PIA? No. We sometimes see more a question, how do you secure the data in the process and there we see questions from the PIA, for security and confidentiality internally but not so much on the process towards the customer on how we are going to use the data.”

Question 9c:”I guess you have the chief data officer or privacy officer who are responsible for the policy around those right?”

Answer 9c – Interviewee J:” We have those yes and I have got every month a data quality board,that is how we call it. But every month we have a discussion as a data owner, with the data stewards together with the departments of the CBO, are we in line with all the policies. Do we see new policies coming up? What are the actions? I think we still have quite some legacy to solve specifically on data quality. We have customers who are already customers for 70 years, there we see sometimes a quality issue.”

Question 10:” A little bit on the IT concepts around data. Do you have data lakes? Because as a concept in the bank they usually conceive it quite different from the GDPR. Because GDPR is about restricting access and data lake to have horizontally access rights to the data. Did you also have to deal with this kind of initiatives? Did you just restrict it to the access aspects or went also to privacy and security by design? ”

Answer 10 – Interviewee J:” The setups of the data lake and the source of record, by default none has access. If organizations, departments or people, most of the times is about organizational processes, want to get access towards data we give them access. That is why I have got two data stewards who are going to provide access so that APIs can be accessed internally by other departments or even when they want to set up a specific part within the data lake to get access for reporting or analysis purposes. Each and every time we have to provide them access and we approve it. The big changes are covered in the user agreements. Sometimes we need the data usage approval, it differs a bit on what is exactly required.”

Question 11:” Do you also use samples of anonymized data or pseudonymized? It’s some sort of encryption so that we do not use the real data that can reveal the identity of the customer.”

Answer 11 – Interviewee j:” we have two systems, in most organization is like that. We have the production database, always with the actual data so you have access to the actual data of our customers. Also for analysis purposes, our data analysts looking at the real data. I honestly believe that we have to do it, otherwise it becomes complicated system. Then we have our development, test and acceptance environment. In the acceptance environment we have specific data masking capability. Once a month we take the dataset from our production database, we scramble into acceptance to make them ready. Then in test where people can mask data and can do their test. And then we can mix and exchange names or read it backwards. So we mix them not to be traceable towards actual customers but still there are real names so people can relate in their test.”

Question 12:” How would you characterize the level of maturity to GDPR compliance?”

Answer 12 – Interviewee J:” If I have to compare us to the market, we are quite advanced. If you look at GDPR it is still evolving in the interpretation and we have to make a few steps. But I think in this market wide, we understand the extent of GDPR for some elements we are overdoing, that again we have to re-engineer to be at the appropriate level and to balance maybe the different interests. For some things we are still evolving like systems which are using are pre-GDPR or medieval times. Privacy by design, is one of the discussions having with internal privacy officers. I think we still need to make some steps for the ancient systems. For example, the data lake which is restricted by design, so you cannot access data unless you have approval for a specific scope of data. We also have assets in our systems where you get with one service, you get access to the full system. It’s really hard to limit there the access to other systems and is not designed with privacy in mind. So I think when we are going to change those applications and make a few steps.”

3. Decoding Outcome of Interview Phase two

3.1 GDPR

The table below summarizes the number of times each keyword or phrase has been mentioned in the interviews and this one is translated into frequency. Interviewee I is excluded from this calculations since he/she did not contribute on the GDPR subject.

Keywords/Key phrases	Additional words /Similar meaning	Focus Topic	D	E	F	G	H	I	J	Total per Keyword/phrase	Frequency
Change(s), heavy, impact, affect	Major, impactful	Impact	N/A	N/A	N/A	2	N/A	N/A	N/A	2	0,167
Continuously Learning sessions, continuous knowledge sessions, trainings	Course, seminars, constantly, repetitive, demand	Training	3	5	5	N/A	2	N/A	1	16	0,833
Multiple departments/disciplinary, jointly, together	Joint, different departments	Training	N/A	2	1	N/A	N/A	N/A	N/A	3	0,333
Awareness,aware, communication	Attention	Impact	4	2	3	3	1	N/A	N/A	13	0,833
In public, society		Impact	N/A	N/A	N/A	1	N/A	N/A	N/A	1	0,167
Mandatory course, mandatory e-learning	required, obligation	Training	2	N/A	1	1	1	N/A	1	6	0,833
Management supervision, control	Higher management/level, monitored	Training	3	2	N/A	N/A	N/A	N/A	N/A	5	0,333
Business Cases, incident analysis	practical examples/appliances, use cases	Training	N/A	2	1	N/A	N/A	N/A	N/A	3	0,333
PIAs, DPIAs, assessments, questionnaire	Questions	Process Assessment	2	2	3	N/A	N/A	N/A	2	9	0,667
On system, per system, on system level		Process Assessment	3	3	1	N/A	N/A	N/A	N/A	7	0,500
On process level, on data processes		Process Assessment	2	1	2	N/A	N/A	N/A	1	6	0,667
Revised PIAs, Revised DPIAs, (Re-)assessment, refine	update, change	Process Assessment	2	1	N/A	N/A	N/A	N/A	1	4	0,500
Yearly review, on yearly basis, every year		Process Assessment	N/A	1	N/A	N/A	N/A	N/A	N/A	1	0,167
GDPR proof, GDPR compliant	In order to comply	IT Implementation	N/A	N/A	N/A	N/A	N/A	N/A	N/A	0	0,000
System implementation, new system		IT Implementation	N/A	N/A	N/A	N/A	N/A	N/A	N/A	0	0,000
Legacy systems, old systems, issues		IT Implementation	N/A	N/A	1	N/A	N/A	N/A	2	3	0,333
Data sanitization, data minimization	Minimum required data	IT Implementation	N/A	N/A	1	N/A	N/A	N/A	N/A	1	0,167
Data encryption, anonymization	Anonymized data, masking, test	IT Implementation	1	1	N/A	N/A	N/A	N/A	4	6	0,500
Data Lake		IT Implementation	N/A	N/A	3	N/A	N/A	N/A	3	6	0,286
In control, Adequate level	Compliant, well, sufficient	Maturity	1	N/A	N/A	1	N/A	N/A	N/A	2	0,333
Maturity Levels	mature, advanced	Maturity	1	N/A	N/A	N/A	N/A	N/A	1	2	0,333
Not mature	insufficient	Maturity	N/A	1	N/A	N/A	N/A	N/A	N/A	1	0,167
BAU, integrated processes, integrated activities		Maturity	N/A	N/A	1	N/A	N/A	N/A	N/A	1	0,167
Obligation	follow, reactive	Maturity	N/A	3	N/A	N/A	N/A	N/A	N/A	3	0,167
Opportunities, Enable		Maturity	1	N/A	N/A	N/A	N/A	N/A	N/A	1	0,167
Further improvement, ongoing, in progress		Maturity	N/A	N/A	N/A	N/A	N/A	N/A	2	2	0,167

3.2 PSD2

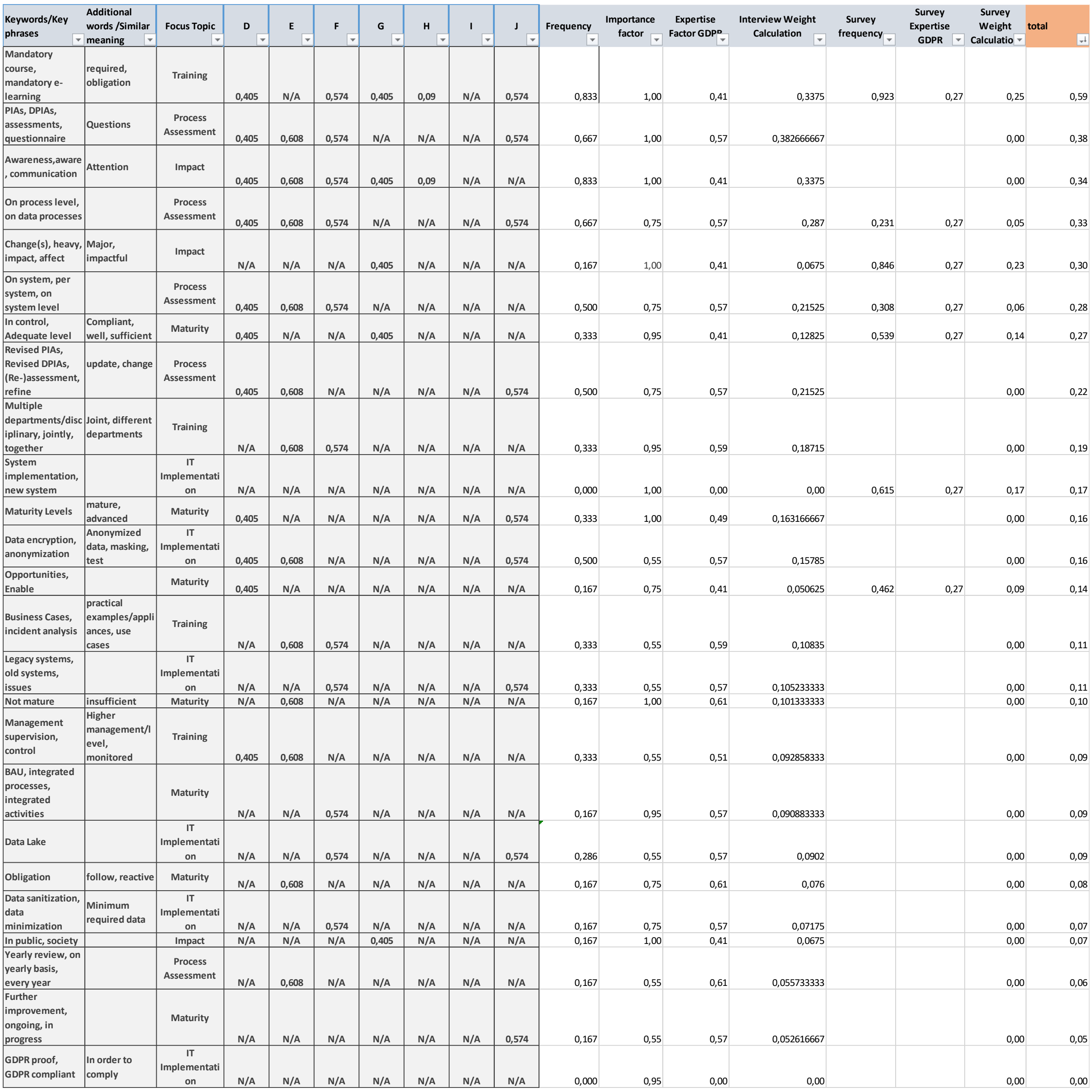
The table below summarizes the number of times each keyword or phrase has been mentioned in the interviews and this one is translated into frequency. Interviewees E and H are excluded from this calculations since they did not contribute on the PSD2 subject.

Keywords/Key phrases	Additional words /Similar meaning	Focus Topic	D	E	F	G	H	I	J	Total per keyword/phrase	Frequency
Learning sessions, seminars, knowledge sessions	Course	Training	N/A	N/A	N/A	N/A	N/A	1	4	5	0,4
Not continuous trainings, limited need	not additional training, not broad	Training	N/A	N/A	2	1	N/A	3	1	7	0,8
Staff/Employees involved, specialists	Specific departments, lesser extent	Training	N/A	N/A	1	1	N/A	N/A	2	4	0,6
System implementation, new system		IT Implementation	N/A	N/A	N/A	N/A	N/A	N/A	N/A	0	0
API implementation, API in place	API based	IT Implementation	1	N/A	2	2	N/A	1	4	10	1
Revised guidelines, revised processes required, impact on API implementation	change, alter	Revised Guidelines	N/A	N/A	3	N/A	N/A	N/A	1	4	0,4
ICT requirements	technical, specifications, standards	Revised Guidelines	4	N/A	N/A	N/A	N/A	N/A	1	5	0,4
Customer Consent		Consent	N/A	N/A	N/A	N/A	N/A	N/A	N/A	0	0
Data Agreements with TTPS	one-sided consent	Consent	N/A	N/A	N/A	N/A	N/A	N/A	N/A	0	0
Market Competition	healthy competition	Competition	N/A	N/A	N/A	N/A	N/A	N/A	N/A	0	0
No Innovation Block	no disruption	Competition	1	N/A	N/A	N/A	N/A	N/A	N/A	1	0,2
Adequate, in control		Maturity	N/A	N/A	N/A	N/A	N/A	1	N/A	1	0,2
Not adequate		Maturity	N/A	N/A	N/A	N/A	N/A	N/A	1	1	0,2
BAU, integrated processes, integrated activities, mature	embedded	Maturity	N/A	N/A	3	1	N/A	N/A	N/A	4	0,4
Further improvement, ongoing, in progress		Maturity	N/A	N/A	N/A	N/A	N/A	N/A	N/A	0	0

4. Total Weight Calculations

4.1 GDPR

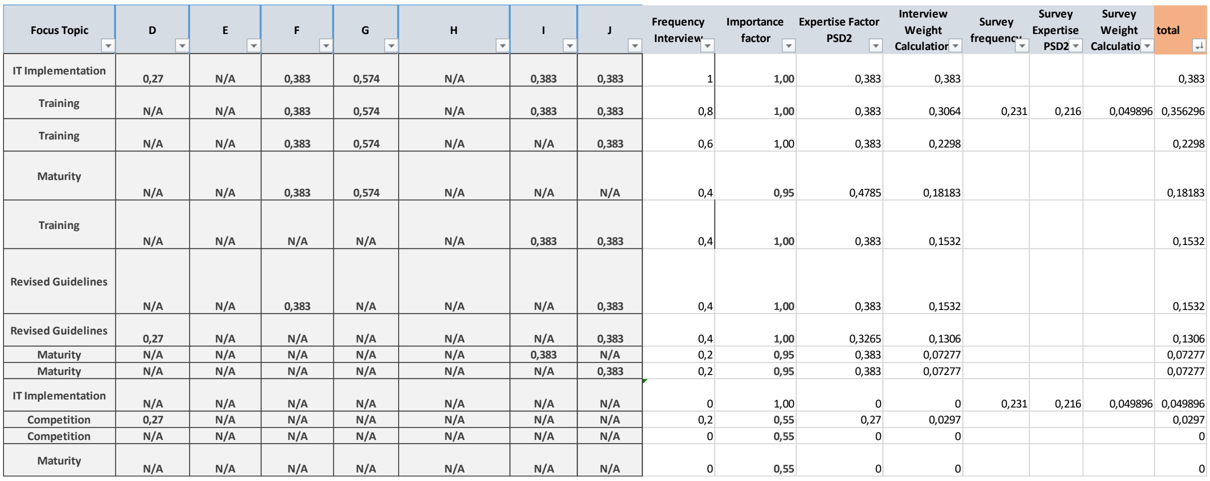
The table below summarizes the calculations for all the GDPR keywords and key phrases. Columns D-J consist of the expertise factor values. The column Total gives the final weight and then they are sorted from the highest to lowest.



Keywords/Key phrases	Additional words /Similar meaning	Focus Topic	D	E	F	G	H	I	J	Frequency	Importance factor	Expertise Factor GDPR	Interview Weight Calculation	Survey frequency	Survey Expertise GDPR	Survey Weight Calculatio	total
Mandatory course, mandatory e-learning	required, obligation	Training	0,405	N/A	0,574	0,405	0,09	N/A	0,574	0,833	1,00	0,41	0,3375	0,923	0,27	0,25	0,59
PIAs, DPIAs, assessments, questionnaire	Questions	Process Assessment	0,405	0,608	0,574	N/A	N/A	N/A	0,574	0,667	1,00	0,57	0,382666667			0,00	0,38
Awareness,aware, communication	Attention	Impact	0,405	0,608	0,574	0,405	0,09	N/A	N/A	0,833	1,00	0,41	0,3375			0,00	0,34
On process level, on data processes		Process Assessment	0,405	0,608	0,574	N/A	N/A	N/A	0,574	0,667	0,75	0,57	0,287	0,231	0,27	0,05	0,33
Change(s), heavy, impact, affect	Major, impactful	Impact	N/A	N/A	N/A	0,405	N/A	N/A	N/A	0,167	1,00	0,41	0,0675	0,846	0,27	0,23	0,30
On system, per system, on system level		Process Assessment	0,405	0,608	0,574	N/A	N/A	N/A	N/A	0,500	0,75	0,57	0,21525	0,308	0,27	0,06	0,28
In control, Adequate level	Compliant, well, sufficient	Maturity	0,405	N/A	N/A	0,405	N/A	N/A	N/A	0,333	0,95	0,41	0,12825	0,539	0,27	0,14	0,27
Revised PIAs, Revised DPIAs, (Re-)assessment, refine	update, change	Process Assessment	0,405	0,608	N/A	N/A	N/A	N/A	0,574	0,500	0,75	0,57	0,21525			0,00	0,22
Multiple departments/disciplinary, jointly, together	Joint, different departments	Training	N/A	0,608	0,574	N/A	N/A	N/A	N/A	0,333	0,95	0,59	0,18715			0,00	0,19
System implementation, new system		IT Implementation	N/A	N/A	N/A	N/A	N/A	N/A	N/A	0,000	1,00	0,00	0,00	0,615	0,27	0,17	0,17
Maturity Levels	mature, advanced	Maturity	0,405	N/A	N/A	N/A	N/A	N/A	0,574	0,333	1,00	0,49	0,163166667			0,00	0,16
Data encryption, anonymization	Anonymized data, masking, test	IT Implementation	0,405	0,608	N/A	N/A	N/A	N/A	0,574	0,500	0,55	0,57	0,15785			0,00	0,16
Opportunities, Enable		Maturity	0,405	N/A	N/A	N/A	N/A	N/A	N/A	0,167	0,75	0,41	0,050625	0,462	0,27	0,09	0,14
Business Cases, incident analysis	practical examples/appliances, use cases	Training	N/A	0,608	0,574	N/A	N/A	N/A	N/A	0,333	0,55	0,59	0,10835			0,00	0,11
Legacy systems, old systems, issues		IT Implementation	N/A	N/A	0,574	N/A	N/A	N/A	0,574	0,333	0,55	0,57	0,105233333			0,00	0,11
Not mature	insufficient	Maturity	N/A	0,608	N/A	N/A	N/A	N/A	N/A	0,167	1,00	0,61	0,101333333			0,00	0,10
Management supervision, control	Higher management/level, monitored	Training	0,405	0,608	N/A	N/A	N/A	N/A	N/A	0,333	0,55	0,51	0,092858333			0,00	0,09
BAU, integrated processes, integrated activities		Maturity	N/A	N/A	0,574	N/A	N/A	N/A	N/A	0,167	0,95	0,57	0,090883333			0,00	0,09
Data Lake		IT Implementation	N/A	N/A	0,574	N/A	N/A	N/A	0,574	0,286	0,55	0,57	0,0902			0,00	0,09
Obligation	follow, reactive	Maturity	N/A	0,608	N/A	N/A	N/A	N/A	N/A	0,167	0,75	0,61	0,076			0,00	0,08
Data sanitization, data minimization	Minimum required data	IT Implementation	N/A	N/A	0,574	N/A	N/A	N/A	N/A	0,167	0,75	0,57	0,07175			0,00	0,07
In public, society		Impact	N/A	N/A	N/A	0,405	N/A	N/A	N/A	0,167	1,00	0,41	0,0675			0,00	0,07
Yearly review, on yearly basis, every year		Process Assessment	N/A	0,608	N/A	N/A	N/A	N/A	N/A	0,167	0,55	0,61	0,055733333			0,00	0,06
Further improvement, ongoing, in progress		Maturity	N/A	N/A	N/A	N/A	N/A	N/A	0,574	0,167	0,55	0,57	0,052616667			0,00	0,05
GDPR proof, GDPR compliant	In order to comply	IT Implementation	N/A	N/A	N/A	N/A	N/A	N/A	N/A	0,000	0,95	0,00	0,00			0,00	0,00

3.4 PSD2

The table below summarizes the calculations for all the PSD2 keywords and key phrases. Columns D-J consist of the expertise factor values. The column total gives the final weight and then they are sorted from the highest to lowest.



Focus Topic	D	E	F	G	H	I	J	Frequency Interview	Importance factor	Expertise Factor PSD2	Interview Weight Calculatior	Survey frequency	Survey Expertise PSD2	Survey Weight Calculatio	total
IT Implementation	0,27	N/A	0,383	0,574	N/A	0,383	0,383	1	1,00	0,383	0,383				0,383
Training	N/A	N/A	0,383	0,574	N/A	0,383	0,383	0,8	1,00	0,383	0,3064	0,231	0,216	0,049896	0,356296
Training	N/A	N/A	0,383	0,574	N/A	N/A	0,383	0,6	1,00	0,383	0,2298				0,2298
Maturity	N/A	N/A	0,383	0,574	N/A	N/A	N/A	0,4	0,95	0,4785	0,18183				0,18183
Training	N/A	N/A	N/A	N/A	N/A	0,383	0,383	0,4	1,00	0,383	0,1532				0,1532
Revised Guidelines	N/A	N/A	0,383	N/A	N/A	N/A	0,383	0,4	1,00	0,383	0,1532				0,1532
Revised Guidelines	0,27	N/A	N/A	N/A	N/A	N/A	0,383	0,4	1,00	0,3265	0,1306				0,1306
Maturity	N/A	N/A	N/A	N/A	N/A	0,383	N/A	0,2	0,95	0,383	0,07277				0,07277
Maturity	N/A	N/A	N/A	N/A	N/A	N/A	0,383	0,2	0,95	0,383	0,07277				0,07277
IT Implementation	N/A	N/A	N/A	N/A	N/A	N/A	N/A	0	1,00	0	0	0,231	0,216	0,049896	0,049896
Competition	0,27	N/A	N/A	N/A	N/A	N/A	N/A	0,2	0,55	0,27	0,0297				0,0297
Competition	N/A	N/A	N/A	N/A	N/A	N/A	N/A	0	0,55	0	0				0
Maturity	N/A	N/A	N/A	N/A	N/A	N/A	N/A	0	0,55	0	0				0

5. Sensitivity Analysis Calculations

5.1 GDPR Scenario 1

Replace Final Expertise factors below 0.49 with value 0.49 which is the median of the Interview GDPR Expertise factor. The column Total gives the Total Weight Outcome and is sorted from the highest to the lowest value.

Keywords/Key phrases	Additional words /Similar meaning	Focus Topic	D	E	F	G	H	I	J	Frequency	Importance factor	Expertise Factor GDPR	Interview Weight Calculation	Survey frequency	Survey Expertise GDPR	Survey Weight Calculation	total
Mandatory course, mandatory e-learning	required, obligation	Training	0,49	N/A	0,574	0,49	0,49	N/A	0,574	0,833	1,00	0,49	0,41	0,923	0,27	0,25	0,66
Awareness,aware, communication	Attention	Impact	0,49	0,608	0,574	0,49	0,49	N/A	N/A	0,833	1,00	0,49	0,41			0,00	0,41
PIAs, DPIAs, assessments, questionnaire	Questions	Process Assessment	0,405	0,608	0,574	N/A	N/A	N/A	0,574	0,667	1,00	0,57	0,38			0,00	0,38
On process level, on data processes		Process Assessment	0,49	0,608	0,574	N/A	N/A	N/A	0,574	0,667	0,75	0,57	0,29	0,231	0,27	0,05	0,33
Change(s), heavy, impact, affect	Major, impactful	Impact	N/A	N/A	N/A	0,49	N/A	N/A	N/A	0,167	1,00	0,49	0,08	0,846	0,27	0,23	0,31
In control, Adequate level	Compliant, well, sufficient	Maturity	0,49	N/A	N/A	0,49	N/A	N/A	N/A	0,333	0,95	0,49	0,16	0,539	0,27	0,14	0,29
On system, per system, on system level		Process Assessment	0,49	0,608	0,574	N/A	N/A	N/A	N/A	0,500	0,75	0,57	0,22	0,308	0,27	0,06	0,28
Revised PIAs, Revised DPIAs, (Re-)assessment, refine	update, change	Process Assessment	0,49	0,608	N/A	N/A	N/A	N/A	0,574	0,500	0,75	0,57	0,22			0,00	0,22
Multiple departments/disciplinary, jointly, together	Joint, different departments	Training	N/A	0,608	0,574	N/A	N/A	N/A	N/A	0,333	0,95	0,59	0,19			0,00	0,19
Maturity Levels	mature, advanced	Maturity	0,49	N/A	N/A	N/A	N/A	N/A	0,574	0,333	1,00	0,53	0,18			0,00	0,18
System implementation, new system		IT Implementation	N/A	N/A	N/A	N/A	N/A	N/A	N/A	0,000	1,00	0,00	0,00	0,615	0,27	0,17	0,17
Data encryption, anonymization	Anonymized data, masking, test	IT Implementation	0,49	0,608	N/A	N/A	N/A	N/A	0,574	0,500	0,55	0,57	0,16			0,00	0,16
Opportunities, Enable		Maturity	0,49	N/A	N/A	N/A	N/A	N/A	N/A	0,167	0,75	0,49	0,06	0,462	0,27	0,09	0,15
Business Cases, incident analysis	practical examples/appliances, use cases	Training	N/A	0,608	0,574	N/A	N/A	N/A	N/A	0,333	0,55	0,59	0,11			0,00	0,11
Legacy systems, old systems, issues		IT Implementation	N/A	N/A	0,574	N/A	N/A	N/A	0,574	0,333	0,55	0,57	0,11			0,00	0,11
Not mature	insufficient	Maturity	N/A	0,608	N/A	N/A	N/A	N/A	N/A	0,167	1,00	0,61	0,10			0,00	0,10
Management supervision, control	Higher management/level, monitored	Training	0,49	0,608	N/A	N/A	N/A	N/A	N/A	0,333	0,55	0,55	0,10			0,00	0,10
BAU, integrated processes, integrated activities		Maturity	N/A	N/A	0,574	N/A	N/A	N/A	N/A	0,167	0,95	0,57	0,09			0,00	0,09
Data Lake		IT Implementation	N/A	N/A	0,574	N/A	N/A	N/A	0,574	0,286	0,55	0,57	0,09			0,00	0,09
In public, society		Impact	N/A	N/A	N/A	0,49	N/A	N/A	N/A	0,167	1,00	0,49	0,08			0,00	0,08
Obligation	follow, reactive	Maturity	N/A	0,608	N/A	N/A	N/A	N/A	N/A	0,167	0,75	0,61	0,08			0,00	0,08
Data sanitization, data minimization	Minimum required data	IT Implementation	N/A	N/A	0,574	N/A	N/A	N/A	N/A	0,167	0,75	0,57	0,07			0,00	0,07
Yearly review, on yearly basis, every year		Process Assessment	N/A	0,608	N/A	N/A	N/A	N/A	N/A	0,167	0,55	0,61	0,06			0,00	0,06
Further improvement, ongoing, in progress		Maturity	N/A	N/A	N/A	N/A	N/A	N/A	0,574	0,167	0,55	0,57	0,05			0,00	0,05
GDPR proof, GDPR compliant	In order to comply	IT Implementation	N/A	N/A	N/A	N/A	N/A	N/A	N/A	0,000	0,95	0,00	0,00			0,00	0,00

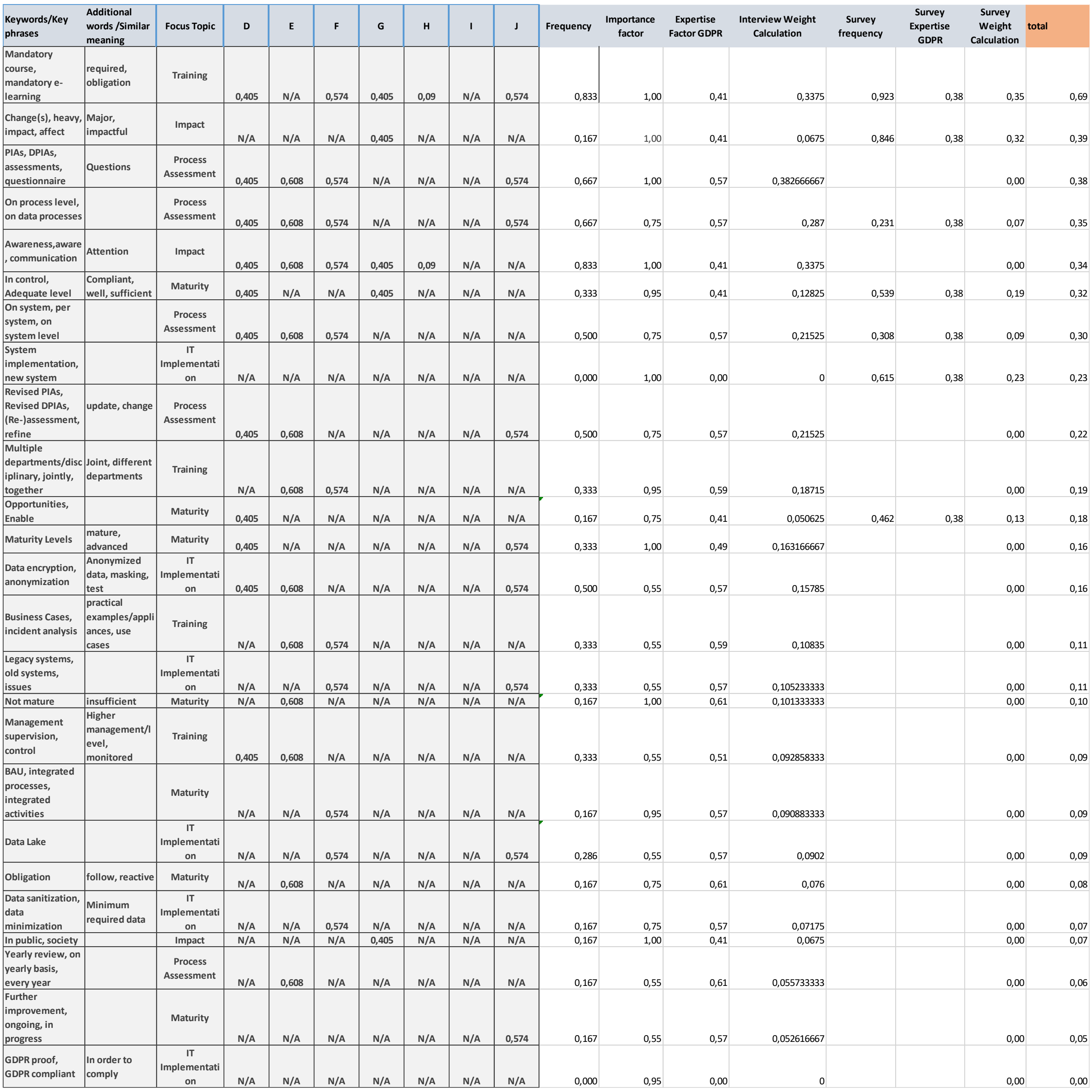
5.2 GDPR Scenario 2

For the interview phase two, Interviewees G & H, who were the less experts in GDPR to be replaced by experts in the sense that the GDPR Expertise Factor to be the maximum with value 0.90.

Keywords/Key phrases	Additional words /Similar meaning	Focus Topic	D	E	F	G	H	I	J	Frequency	Importance factor	Expertise Factor GDPR	Interview Weight Calculation	Survey frequency	Survey Expertise GDPR	Survey Weight Calculation	total
Mandatory course, mandatory e-learning	required, obligation	Training	0,405	N/A	0,574	0,608	0,324	N/A	0,574	0,833	1,00	0,57	0,478333333	0,923	0,27	0,25	0,73
Awareness,aware, communication	Attention	Impact	0,405	0,608	0,574	0,608	0,324	N/A	N/A	0,833	1,00	0,57	0,478333333			0,00	0,48
PIAs, DPIAs, assessments, questionnaire	Questions	Process Assessment	0,405	0,608	0,574	N/A	N/A	N/A	0,574	0,667	1,00	0,57	0,382666667			0,00	0,38
On process level, on data processes		Process Assessment	0,405	0,608	0,574	N/A	N/A	N/A	0,574	0,667	0,75	0,57	0,287	0,231	0,27	0,05	0,33
Change(s), heavy, impact, affect	Major, impactful	Impact	N/A	N/A	N/A	0,608	N/A	N/A	N/A	0,167	1,00	0,61	0,101333333	0,846	0,27	0,23	0,33
In control, Adequate level	Compliant, well, sufficient	Maturity	0,405	N/A	N/A	0,608	N/A	N/A	N/A	0,333	0,95	0,51	0,160391667	0,539	0,27	0,14	0,30
On system, per system, on system level		Process Assessment	0,405	0,608	0,574	N/A	N/A	N/A	N/A	0,500	0,75	0,57	0,21525	0,308	0,27	0,06	0,28
Revised PIAs, Revised DPIAs, (Re-)assessment, refine	update, change	Process Assessment	0,405	0,608	N/A	N/A	N/A	N/A	0,574	0,500	0,75	0,57	0,21525			0,00	0,22
Multiple departments/disciplinary, jointly, together	Joint, different departments	Training	N/A	0,608	0,574	N/A	N/A	N/A	N/A	0,333	0,95	0,59	0,18715			0,00	0,19
System implementation, new system		IT Implementation	N/A	N/A	N/A	N/A	N/A	N/A	N/A	0,000	1,00	0,00	0,00	0,615	0,27	0,17	0,17
Maturity Levels	mature, advanced	Maturity	0,405	N/A	N/A	N/A	N/A	N/A	0,574	0,333	1,00	0,49	0,163166667			0,00	0,16
Data encryption, anonymization	Anonymized data, masking, test	IT Implementation	0,405	0,608	N/A	N/A	N/A	N/A	0,574	0,500	0,55	0,57	0,15785			0,00	0,16
Opportunities, Enable		Maturity	0,405	N/A	N/A	N/A	N/A	N/A	N/A	0,167	0,75	0,41	0,050625	0,462	0,27	0,09	0,14
Business Cases, incident analysis	practical examples/appliances, use cases	Training	N/A	0,608	0,574	N/A	N/A	N/A	N/A	0,333	0,55	0,59	0,10835			0,00	0,11
Legacy systems, old systems, issues		IT Implementation	N/A	N/A	0,574	N/A	N/A	N/A	0,574	0,333	0,55	0,57	0,105233333			0,00	0,11
Not mature	insufficient	Maturity	N/A	0,608	N/A	N/A	N/A	N/A	N/A	0,167	1,00	0,61	0,101333333			0,00	0,10
In public, society		Impact	N/A	N/A	N/A	0,608	N/A	N/A	N/A	0,167	1,00	0,61	0,101333333			0,00	0,10
Management supervision, control	Higher management/level, monitored	Training	0,405	0,608	N/A	N/A	N/A	N/A	N/A	0,333	0,55	0,51	0,092858333			0,00	0,09
BAU, integrated processes, integrated activities		Maturity	N/A	N/A	0,574	N/A	N/A	N/A	N/A	0,167	0,95	0,57	0,090883333			0,00	0,09
Data Lake		IT Implementation	N/A	N/A	0,574	N/A	N/A	N/A	0,574	0,286	0,55	0,57	0,0902			0,00	0,09
Obligation	follow, reactive	Maturity	N/A	0,608	N/A	N/A	N/A	N/A	N/A	0,167	0,75	0,61	0,076			0,00	0,08
Data sanitization, data minimization	Minimum required data	IT Implementation	N/A	N/A	0,574	N/A	N/A	N/A	N/A	0,167	0,75	0,57	0,07175			0,00	0,07
Yearly review, on yearly basis, every year		Process Assessment	N/A	0,608	N/A	N/A	N/A	N/A	N/A	0,167	0,55	0,61	0,055733333			0,00	0,06
Further improvement, ongoing, in progress		Maturity	N/A	N/A	N/A	N/A	N/A	N/A	0,574	0,167	0,55	0,57	0,052616667			0,00	0,05
GDPR proof, GDPR compliant	In order to comply	IT Implementation	N/A	N/A	N/A	N/A	N/A	N/A	N/A	0,000	0,95	0,00	0,00			0,00	0,00

5.3 GDPR Scenario 3

For the online questionnaire participants we increased the expertise factor from 0.27 to 0.38 which is the median value of 0.27 and 0.49, between the interview and the survey expertise factor. The value is replaced in Column Survey Expertise GDPR.



Keywords/Key phrases	Additional words /Similar meaning	Focus Topic	D	E	F	G	H	I	J	Frequency	Importance factor	Expertise Factor GDPR	Interview Weight Calculation	Survey frequency	Survey Expertise GDPR	Survey Weight Calculation	total
Mandatory course, mandatory e-learning	required, obligation	Training	0,405	N/A	0,574	0,405	0,09	N/A	0,574	0,833	1,00	0,41	0,3375	0,923	0,38	0,35	0,69
Change(s), heavy, impact, affect	Major, impactful	Impact	N/A	N/A	N/A	0,405	N/A	N/A	N/A	0,167	1,00	0,41	0,0675	0,846	0,38	0,32	0,39
PIAs, DPIAs, assessments, questionnaire	Questions	Process Assessment	0,405	0,608	0,574	N/A	N/A	N/A	0,574	0,667	1,00	0,57	0,382666667			0,00	0,38
On process level, on data processes		Process Assessment	0,405	0,608	0,574	N/A	N/A	N/A	0,574	0,667	0,75	0,57	0,287	0,231	0,38	0,07	0,35
Awareness,aware, communication	Attention	Impact	0,405	0,608	0,574	0,405	0,09	N/A	N/A	0,833	1,00	0,41	0,3375			0,00	0,34
In control, Adequate level	Compliant, well, sufficient	Maturity	0,405	N/A	N/A	0,405	N/A	N/A	N/A	0,333	0,95	0,41	0,12825	0,539	0,38	0,19	0,32
On system, per system, on system level		Process Assessment	0,405	0,608	0,574	N/A	N/A	N/A	N/A	0,500	0,75	0,57	0,21525	0,308	0,38	0,09	0,30
System implementation, new system		IT Implementation	N/A	N/A	N/A	N/A	N/A	N/A	N/A	0,000	1,00	0,00	0	0,615	0,38	0,23	0,23
Revised PIAs, Revised DPIAs, (Re-)assessment, refine	update, change	Process Assessment	0,405	0,608	N/A	N/A	N/A	N/A	0,574	0,500	0,75	0,57	0,21525			0,00	0,22
Multiple departments/disciplinary, jointly, together	Joint, different departments	Training	N/A	0,608	0,574	N/A	N/A	N/A	N/A	0,333	0,95	0,59	0,18715			0,00	0,19
Opportunities, Enable		Maturity	0,405	N/A	N/A	N/A	N/A	N/A	N/A	0,167	0,75	0,41	0,050625	0,462	0,38	0,13	0,18
Maturity Levels	mature, advanced	Maturity	0,405	N/A	N/A	N/A	N/A	N/A	0,574	0,333	1,00	0,49	0,163166667			0,00	0,16
Data encryption, anonymization	Anonymized data, masking, test	IT Implementation	0,405	0,608	N/A	N/A	N/A	N/A	0,574	0,500	0,55	0,57	0,15785			0,00	0,16
Business Cases, incident analysis	practical examples/appliances, use cases	Training	N/A	0,608	0,574	N/A	N/A	N/A	N/A	0,333	0,55	0,59	0,10835			0,00	0,11
Legacy systems, old systems, issues		IT Implementation	N/A	N/A	0,574	N/A	N/A	N/A	0,574	0,333	0,55	0,57	0,105233333			0,00	0,11
Not mature	insufficient	Maturity	N/A	0,608	N/A	N/A	N/A	N/A	N/A	0,167	1,00	0,61	0,101333333			0,00	0,10
Management supervision, control	Higher management/level, monitored	Training	0,405	0,608	N/A	N/A	N/A	N/A	N/A	0,333	0,55	0,51	0,092858333			0,00	0,09
BAU, integrated processes, integrated activities		Maturity	N/A	N/A	0,574	N/A	N/A	N/A	N/A	0,167	0,95	0,57	0,090883333			0,00	0,09
Data Lake		IT Implementation	N/A	N/A	0,574	N/A	N/A	N/A	0,574	0,286	0,55	0,57	0,0902			0,00	0,09
Obligation	follow, reactive	Maturity	N/A	0,608	N/A	N/A	N/A	N/A	N/A	0,167	0,75	0,61	0,076			0,00	0,08
Data sanitization, data minimization	Minimum required data	IT Implementation	N/A	N/A	0,574	N/A	N/A	N/A	N/A	0,167	0,75	0,57	0,07175			0,00	0,07
In public, society		Impact	N/A	N/A	N/A	0,405	N/A	N/A	N/A	0,167	1,00	0,41	0,0675			0,00	0,07
Yearly review, on yearly basis, every year		Process Assessment	N/A	0,608	N/A	N/A	N/A	N/A	N/A	0,167	0,55	0,61	0,055733333			0,00	0,06
Further improvement, ongoing, in progress		Maturity	N/A	N/A	N/A	N/A	N/A	N/A	0,574	0,167	0,55	0,57	0,052616667			0,00	0,05
GDPR proof, GDPR compliant	In order to comply	IT Implementation	N/A	N/A	N/A	N/A	N/A	N/A	N/A	0,000	0,95	0,00	0			0,00	0,00

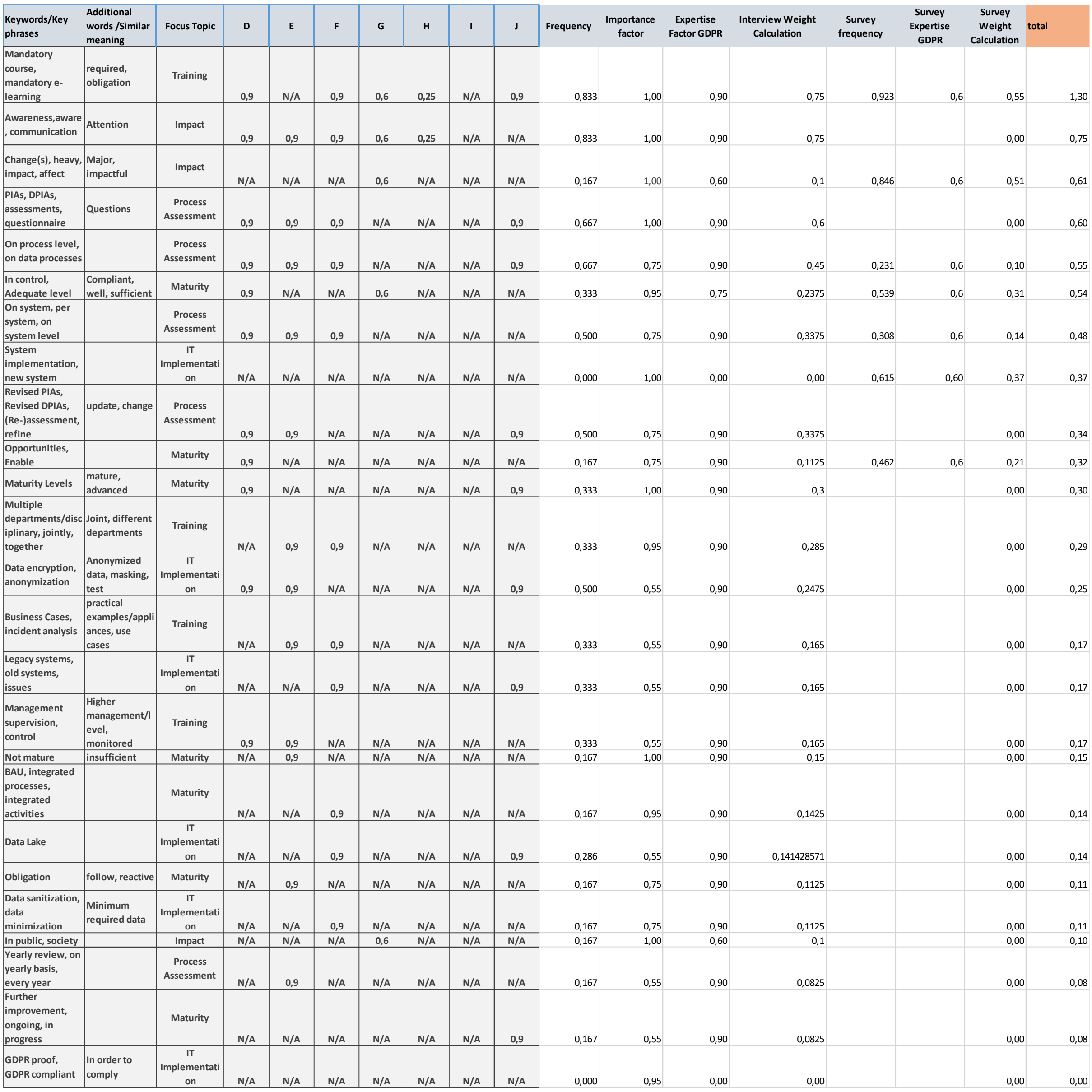
5.4 GDPR Scenario 4

For all the participants in the online survey and the second interview round we remove the background and FI type factors.

The demographics table is adjusted as per below:

	Code	Role	Background	Financial Services Domain	Expertise GDPR	Final Expertise factor GDPR
Interview round two	D	Data Privacy Officer	N/A	N/A	0,90	0,900
	E	Expert Consultant GDPR	N/A	N/A	0,90	0,900
	F	Data Privacy Officer/Data Protection Officer	N/A	N/A	0,90	0,900
	G	Legal Counsel	N/A	N/A	0,60	0,600
	H	Legal Counsel	N/A	N/A	0,25	0,250
	I	Program Manager for Change	N/A	N/A	N/A	N/A
	J	Product Area Lead in Customer Data	N/A	N/A	0,90	0,900
online survey	1		N/A	N/A	0,6	0,600
	2		N/A	N/A	0,6	0,600
	3		N/A	N/A	0,6	0,600
	4		N/A	N/A	0,6	0,600
	5		N/A	N/A	N/A	N/A
	6		N/A	N/A	0,25	0,250
	7		N/A	N/A	0,6	0,600
	8		N/A	N/A	N/A	N/A
	9		N/A	N/A	0,6	0,600
	10		N/A	N/A	N/A	N/A
	11		N/A	N/A	N/A	N/A
	12		N/A	N/A	0,6	0,600
	13		N/A	N/A	0,6	0,600

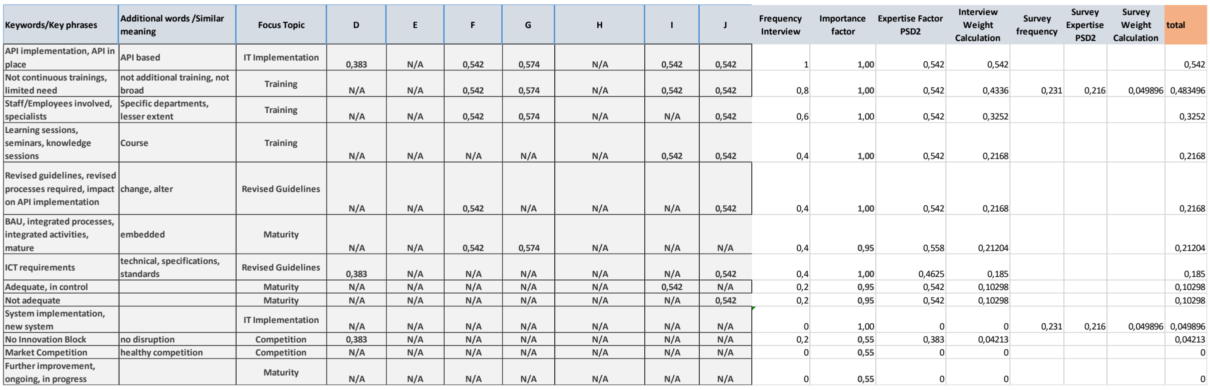
The detailed calculations are as such and sorted on the column Total:



Keywords/Key phrases	Additional words /Similar meaning	Focus Topic	D	E	F	G	H	I	J	Frequency	Importance factor	Expertise Factor GDPR	Interview Weight Calculation	Survey frequency	Survey Expertise GDPR	Survey Weight Calculation	total
Mandatory course, mandatory e-learning	required, obligation	Training	0,9	N/A	0,9	0,6	0,25	N/A	0,9	0,833	1,00	0,90	0,75	0,923	0,6	0,55	1,30
Awareness,aware, communication	Attention	Impact	0,9	0,9	0,9	0,6	0,25	N/A	N/A	0,833	1,00	0,90	0,75			0,00	0,75
Change(s), heavy, impact, affect	Major, impactful	Impact	N/A	N/A	N/A	0,6	N/A	N/A	N/A	0,167	1,00	0,60	0,1	0,846	0,6	0,51	0,61
PIAs, DPIAs, assessments, questionnaire	Questions	Process Assessment	0,9	0,9	0,9	N/A	N/A	N/A	0,9	0,667	1,00	0,90	0,6			0,00	0,60
On process level, on data processes		Process Assessment	0,9	0,9	0,9	N/A	N/A	N/A	0,9	0,667	0,75	0,90	0,45	0,231	0,6	0,10	0,55
In control, Adequate level	Compliant, well, sufficient	Maturity	0,9	N/A	N/A	0,6	N/A	N/A	N/A	0,333	0,95	0,75	0,2375	0,539	0,6	0,31	0,54
On system, per system, on system level		Process Assessment	0,9	0,9	0,9	N/A	N/A	N/A	N/A	0,500	0,75	0,90	0,3375	0,308	0,6	0,14	0,48
System implementation, new system		IT Implementation	N/A	N/A	N/A	N/A	N/A	N/A	N/A	0,000	1,00	0,00	0,00	0,615	0,60	0,37	0,37
Revised PIAs, Revised DPIAs, (Re-)assessment, refine	update, change	Process Assessment	0,9	0,9	N/A	N/A	N/A	N/A	0,9	0,500	0,75	0,90	0,3375			0,00	0,34
Opportunities, Enable		Maturity	0,9	N/A	N/A	N/A	N/A	N/A	N/A	0,167	0,75	0,90	0,1125	0,462	0,6	0,21	0,32
Maturity Levels	mature, advanced	Maturity	0,9	N/A	N/A	N/A	N/A	N/A	0,9	0,333	1,00	0,90	0,3			0,00	0,30
Multiple departments/disciplinary, jointly, together	Joint, different departments	Training	N/A	0,9	0,9	N/A	N/A	N/A	N/A	0,333	0,95	0,90	0,285			0,00	0,29
Data encryption, anonymization	Anonymized data, masking, test	IT Implementation	0,9	0,9	N/A	N/A	N/A	N/A	0,9	0,500	0,55	0,90	0,2475			0,00	0,25
Business Cases, incident analysis	practical examples/appliances, use cases	Training	N/A	0,9	0,9	N/A	N/A	N/A	N/A	0,333	0,55	0,90	0,165			0,00	0,17
Legacy systems, old systems, issues		IT Implementation	N/A	N/A	0,9	N/A	N/A	N/A	0,9	0,333	0,55	0,90	0,165			0,00	0,17
Management supervision, control	Higher management/level, monitored	Training	0,9	0,9	N/A	N/A	N/A	N/A	N/A	0,333	0,55	0,90	0,165			0,00	0,17
Not mature	insufficient	Maturity	N/A	0,9	N/A	N/A	N/A	N/A	N/A	0,167	1,00	0,90	0,15			0,00	0,15
BAU, integrated processes, integrated activities		Maturity	N/A	N/A	0,9	N/A	N/A	N/A	N/A	0,167	0,95	0,90	0,1425			0,00	0,14
Data Lake		IT Implementation	N/A	N/A	0,9	N/A	N/A	N/A	0,9	0,286	0,55	0,90	0,141428571			0,00	0,14
Obligation	follow, reactive	Maturity	N/A	0,9	N/A	N/A	N/A	N/A	N/A	0,167	0,75	0,90	0,1125			0,00	0,11
Data sanitization, data minimization	Minimum required data	IT Implementation	N/A	N/A	0,9	N/A	N/A	N/A	N/A	0,167	0,75	0,90	0,1125			0,00	0,11
In public, society		Impact	N/A	N/A	N/A	0,6	N/A	N/A	N/A	0,167	1,00	0,60	0,1			0,00	0,10
Yearly review, on yearly basis, every year		Process Assessment	N/A	0,9	N/A	N/A	N/A	N/A	N/A	0,167	0,55	0,90	0,0825			0,00	0,08
Further improvement, ongoing, in progress		Maturity	N/A	N/A	N/A	N/A	N/A	N/A	0,9	0,167	0,55	0,90	0,0825			0,00	0,08
GDPR proof, GDPR compliant	In order to comply	IT Implementation	N/A	N/A	N/A	N/A	N/A	N/A	N/A	0,000	0,95	0,00	0,00			0,00	0,00

5.5 PSD2 Scenario 1

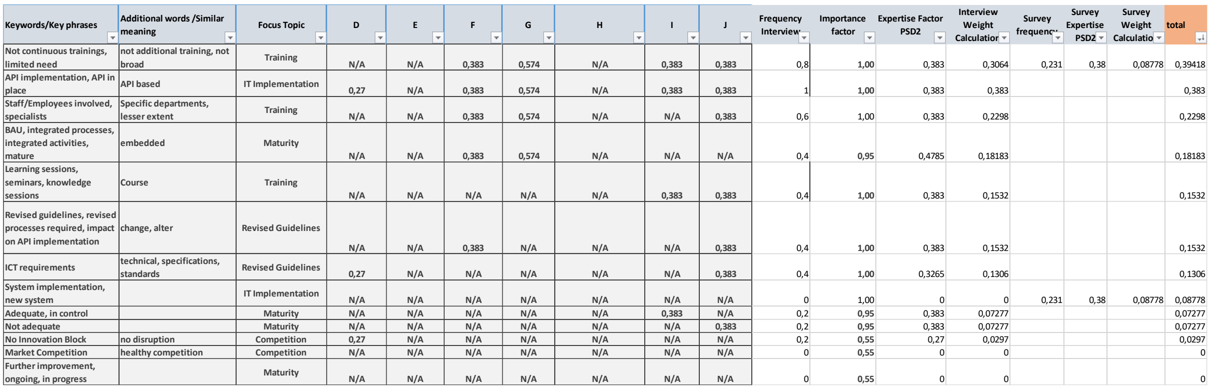
For the interview phase two, Interviewees D,F,I, J , who were the less experts in GDPR to be replaced by experts in the sense that the PSD2 Expertise Factor to be the maximum with value 0.85.



Keywords/Key phrases	Additional words /Similar meaning	Focus Topic	D	E	F	G	H	I	J	Frequency Interview	Importance factor	Expertise Factor PSD2	Interview Weight Calculation	Survey frequency	Survey Expertise PSD2	Survey Weight Calculation	total
API implementation, API in place	API based	IT Implementation	0,383	N/A	0,542	0,574	N/A	0,542	0,542	1	1,00	0,542	0,542				0,542
Not continuous trainings, limited need	not additional training, not broad	Training	N/A	N/A	0,542	0,574	N/A	0,542	0,542	0,8	1,00	0,542	0,4336	0,231	0,216	0,049896	0,483496
Staff/Employees involved, specialists	Specific departments, lesser extent	Training	N/A	N/A	0,542	0,574	N/A	N/A	0,542	0,6	1,00	0,542	0,3252				0,3252
Learning sessions, seminars, knowledge sessions	Course	Training	N/A	N/A	N/A	N/A	N/A	0,542	0,542	0,4	1,00	0,542	0,2168				0,2168
Revised guidelines, revised processes required, impact on API implementation	change, alter	Revised Guidelines	N/A	N/A	0,542	N/A	N/A	N/A	0,542	0,4	1,00	0,542	0,2168				0,2168
BAU, integrated processes, integrated activities, mature	embedded	Maturity	N/A	N/A	0,542	0,574	N/A	N/A	N/A	0,4	0,95	0,558	0,21204				0,21204
ICT requirements	technical, specifications, standards	Revised Guidelines	0,383	N/A	N/A	N/A	N/A	N/A	0,542	0,4	1,00	0,4625	0,185				0,185
Adequate, in control		Maturity	N/A	N/A	N/A	N/A	N/A	0,542	N/A	0,2	0,95	0,542	0,10298				0,10298
Not adequate		Maturity	N/A	N/A	N/A	N/A	N/A	N/A	0,542	0,2	0,95	0,542	0,10298				0,10298
System implementation, new system		IT Implementation	N/A	N/A	N/A	N/A	N/A	N/A	N/A	0	1,00	0	0	0,231	0,216	0,049896	0,049896
No Innovation Block	no disruption	Competition	0,383	N/A	N/A	N/A	N/A	N/A	N/A	0,2	0,55	0,383	0,04213				0,04213
Market Competition	healthy competition	Competition	N/A	N/A	N/A	N/A	N/A	N/A	N/A	0	0,55	0	0				0
Further improvement, ongoing, in progress		Maturity	N/A	N/A	N/A	N/A	N/A	N/A	N/A	0	0,55	0	0				0

5.6 PSD2 Scenario 2

For the online questionnaire participants we increased the expertise factor from 0.27 to 0.38 which is the median value of 0.22 and 0.54, between the interview and the survey expertise factor. The value is replaced in Column Survey Expertise PSD2.



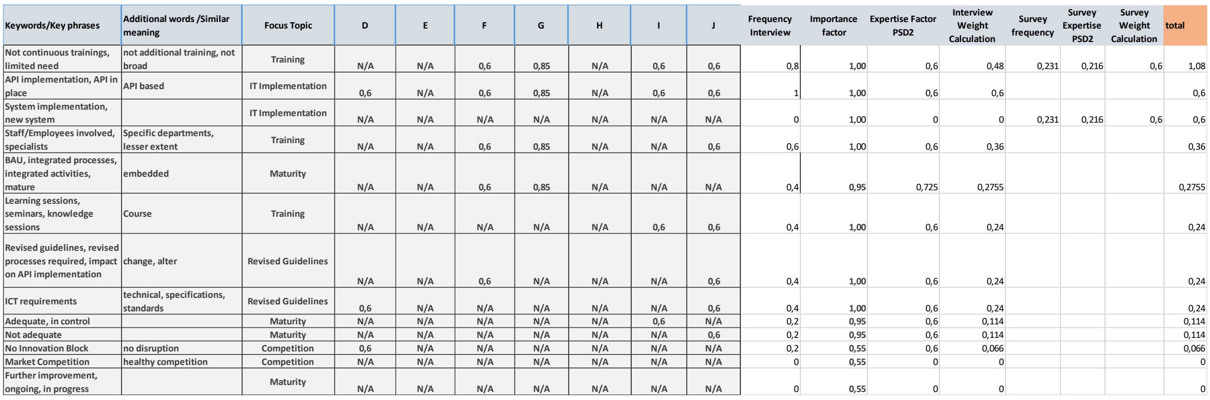
Keywords/Key phrases	Additional words /Similar meaning	Focus Topic	D	E	F	G	H	I	J	Frequency Interview	Importance factor	Expertise Factor PSD2	Interview Weight Calculatior	Survey frequenc	Survey Expertise PSD2	Survey Weight Calculatio	total
Not continuous trainings, limited need	not additional training, not broad	Training	N/A	N/A	0,383	0,574	N/A	0,383	0,383	0,8	1,00	0,383	0,3064	0,231	0,38	0,08778	0,39418
API implementation, API in place	API based	IT Implementation	0,27	N/A	0,383	0,574	N/A	0,383	0,383	1	1,00	0,383	0,383				0,383
Staff/Employees involved, specialists	Specific departments, lesser extent	Training	N/A	N/A	0,383	0,574	N/A	N/A	0,383	0,6	1,00	0,383	0,2298				0,2298
BAU, integrated processes, integrated activities, mature	embedded	Maturity	N/A	N/A	0,383	0,574	N/A	N/A	N/A	0,4	0,95	0,4785	0,18183				0,18183
Learning sessions, seminars, knowledge sessions	Course	Training	N/A	N/A	N/A	N/A	N/A	0,383	0,383	0,4	1,00	0,383	0,1532				0,1532
Revised guidelines, revised processes required, impact on API implementation	change, alter	Revised Guidelines	N/A	N/A	0,383	N/A	N/A	N/A	0,383	0,4	1,00	0,383	0,1532				0,1532
ICT requirements	technical, specifications, standards	Revised Guidelines	0,27	N/A	N/A	N/A	N/A	N/A	0,383	0,4	1,00	0,3265	0,1306				0,1306
System implementation, new system		IT Implementation	N/A	N/A	N/A	N/A	N/A	N/A	N/A	0	1,00	0	0	0,231	0,38	0,08778	0,08778
Adequate, in control		Maturity	N/A	N/A	N/A	N/A	N/A	0,383	N/A	0,2	0,95	0,383	0,07277				0,07277
Not adequate		Maturity	N/A	N/A	N/A	N/A	N/A	N/A	0,383	0,2	0,95	0,383	0,07277				0,07277
No Innovation Block	no disruption	Competition	0,27	N/A	N/A	N/A	N/A	N/A	N/A	0,2	0,55	0,27	0,0297				0,0297
Market Competition	healthy competition	Competition	N/A	N/A	N/A	N/A	N/A	N/A	N/A	0	0,55	0	0				0
Further improvement, ongoing, in progress		Maturity	N/A	N/A	N/A	N/A	N/A	N/A	N/A	0	0,55	0	0				0

5.7 PSD2 Scenario 3

For all the participants in the online survey and the interview round two, we removed the background and the FI type expertise factors. The Final Expertise Factor PSD2 table is adjusted as such:

	Code	**Role**	**Background**	**Financial Services Domain**	**Expertise PSD2**	**Final Expertise Factor PSD2**
Interview round two	D	Data Privacy Officer	N/A	N/A	0,60	0,600
	E	Expert Consultant GDPR	N/A	N/A	N/A	N/A
	F	Data Privacy Officer/Data Protection Officer	N/A	N/A	0,60	0,600
	G	Legal Counsel	N/A	N/A	0,85	0,850
	H	Legal Counsel	N/A	N/A	N/A	N/A
	I	Program Manager for Change	N/A	N/A	0,60	0,600
	J	Product Area Lead in Customer Data	N/A	N/A	0,60	0,600
online survey	1		N/A	N/A	N/A	N/A
	2		N/A	N/A	0,6	0,600
	3		N/A	N/A	N/A	N/A
	4		N/A	N/A	N/A	N/A
	5		N/A	N/A	0,6	0,600
	6		N/A	N/A	N/A	N/A
	7		N/A	N/A	N/A	N/A
	8		N/A	N/A	0,25	0,250
	9		N/A	N/A	N/A	N/A
	10		N/A	N/A	0,6	0,600
	11		N/A	N/A	0,6	0,600
	12		N/A	N/A	0,6	0,600
	13		N/A	N/A	N/A	N/A

Below the detailed calculations are presented, and sorted on the Column Total.



Keywords/Key phrases	Additional words /Similar meaning	Focus Topic	D	E	F	G	H	I	J	Frequency Interview	Importance factor	Expertise Factor PSD2	Interview Weight Calculation	Survey frequency	Survey Expertise PSD2	Survey Weight Calculation	total
Not continuous trainings, limited need	not additional training, not broad	Training	N/A	N/A	0,6	0,85	N/A	0,6	0,6	0,8	1,00	0,6	0,48	0,231	0,216	0,6	1,08
API implementation, API in place	API based	IT Implementation	0,6	N/A	0,6	0,85	N/A	0,6	0,6	1	1,00	0,6	0,6				0,6
System implementation, new system		IT Implementation	N/A	N/A	N/A	N/A	N/A	N/A	N/A	0	1,00	0	0	0,231	0,216	0,6	0,6
Staff/Employees involved, specialists	Specific departments, lesser extent	Training	N/A	N/A	0,6	0,85	N/A	N/A	0,6	0,6	1,00	0,6	0,36				0,36
BAU, integrated processes, integrated activities, mature	embedded	Maturity	N/A	N/A	0,6	0,85	N/A	N/A	N/A	0,4	0,95	0,725	0,2755				0,2755
Learning sessions, seminars, knowledge sessions	Course	Training	N/A	N/A	N/A	N/A	N/A	0,6	0,6	0,4	1,00	0,6	0,24				0,24
Revised guidelines, revised processes required, impact on API implementation	change, alter	Revised Guidelines	N/A	N/A	0,6	N/A	N/A	N/A	0,6	0,4	1,00	0,6	0,24				0,24
ICT requirements	technical, specifications, standards	Revised Guidelines	0,6	N/A	N/A	N/A	N/A	N/A	0,6	0,4	1,00	0,6	0,24				0,24
Adequate, in control		Maturity	N/A	N/A	N/A	N/A	N/A	0,6	N/A	0,2	0,95	0,6	0,114				0,114
Not adequate		Maturity	N/A	N/A	N/A	N/A	N/A	N/A	0,6	0,2	0,95	0,6	0,114				0,114
No Innovation Block	no disruption	Competition	0,6	N/A	N/A	N/A	N/A	N/A	N/A	0,2	0,55	0,6	0,066				0,066
Market Competition	healthy competition	Competition	N/A	N/A	N/A	N/A	N/A	N/A	N/A	0	0,55	0	0				0
Further improvement, ongoing, in progress		Maturity	N/A	N/A	N/A	N/A	N/A	N/A	N/A	0	0,55	0	0				0