Deliverable 1.4

Activity report and results of the testing phase of the living lab process (Delphi survey)

05-06-2022

Project Name: Digital (R)evolution in Belgian Federal Government: An Open Governance Ecosystem for Big Data, Artificial Intelligence, and Blockchain.

Funding Programme: BRAIN-be 2.0 Call 2019

Contract Number: B2/191/P3/DIGI4FED

Work Package: WP1

Author(s): Dr. Mathias Sabbe; Prof Dr. Catherine Fallon

The DIGI4FED consortium consists of the following partners:

KU Leuven (KUL)

UNamur (UN)

UAntwerpen (UA)

ULiége (UL)

Executive Summary

This deliverable presents an activity report for the testing phase of the living lab process which was conducted with the help of a Delphi survey. Most importantly, this survey was devised as a way to test the validity of our design artefact presented in D3.3. (a governance model for the use of new digital technologies in the fight against fraud in the social security and taxation domain). The deliverable is divided into three parts. The first part presents the activity report concerning the Delphi survey: the method, the design, the conduct of the survey, and the survey participants. The second part presents the main results of an analysis of participants' answers to this survey. The collected data was analyzed with the help of simple descriptive statistics as well as qualitative analysis techniques (thematic analysis). The third part elaborates on the assessment of our design artefact according to the survey results and the evaluation criteria that were selected in D3.3. Testing suggests that our proposed model respects all our selected evaluation criteria. The main findings of the qualitative analysis are as follows: 1) Technical solutions alone (e.g., digital wallet solutions, decentralized approaches) would not support citizen trust; 2. The collaboration with private actors appears as a much-needed compromise; 3. Working in networks might foster interoperability and mitigate resource limitations; 4. There is no clear consensus among stakeholders regarding the choice between centralized and decentralized approaches (or a mix of both); 5. Relying on a "regulatory sandbox" approach might help in producing a clear, transparent, and adaptive legal framework; 6. The central role of federal authorities in data governance and the need to associate civil society representatives to governance choices.

TABLE DES MATIERES

List of Figures & Tables 5

List of Acronyms 7

1. Introduction 8

2. The Delphi survey 9

2.1. The Delphi method 9

2.2. Designing and conducting the survey 11

2.3. Survey participants 14

3. Analysis of the collected data 15

3.1. Section 1 - Fostering citizen trust 16

Question 1.1 16

Question 1.2 19

Question 1.3 22

3.2. Section 2 - Promoting coordination and interoperability between administrations 25

Question 2.1 26

Question 2.2 29

Question 2.3 32

Question 2.4 35

3.3. Section 3 - Limiting public actors' dependance towards private actors 37

Question 3.1 37

Question 3.2 40

Question 3.3 43

3.4. Section 4 - Values and data governance 45

Question 4.1 46

Question 4.2 48

Question 4.3 50

Question 4.4 52

3.5. Section 5 - Improving the explainability of the analysis process 54

Question 5.1 55

Question 5.2 58

Question 5.3 60

3.6. Section 6 - Ensuring the legal compliance of the system 61

Question 6.1 62

Question 6.2 64

Question 6.3 66

3.7. Additional Elements 68

4. Model testing 70

4.1. Overall Efficacy 71
4.2. Overall Suitability 73
4.3. Feasibility 76
4.4. Stakeholder endorsement 77
4.5. Cognitive aspects 78
4.6. Overall consistency 79
4.7. Overall simplicity 80
4.8. Sustainability 81
5. General synthesis and conclusion 84
Synthesis of the main results of the survey 84
Synthesis of model testing 90
General conclusion of the deliverable 93
6. References 95

LIST OF FIGURES & TABLES

Figure 1 – Question 1.1 summary: do these solutions provide an effective response to the lack of citizen trust? 17

Figure 2 - Tag cloud for question 1.1 19

Figure 3 – Question 1.2 summary: are digital wallets an adequate solution to a lack of citizen trust? 20

Figure 4 - Tag cloud for question 1.2 22

Figure 5 - Question 1.3 summary: is decentralized data management an appropriate response to a lack of citizen trust? 23

Figure 6- Tag cloud for question 1.3 25

Figure 7- Tag cloud for question 2.1 29

Figure 8 - Question 2.2 summary: can these solutions help overcome interoperability and coordination issues? 29

Figure 9 - Tag cloud for question 2.2 32

Figure 10- Question 2.3 summary: is a data exchange platform between administrations feasible? 33

Figure 11 - Tag cloud for question 2.3 34

Figure 12 - Tag cloud for question 2.4 36

Figure 13 - Question 3.1 summary: do these solutions limit the dependence of public actors? 38

Figure 14 - Tag cloud for question 3.1 40

Figure 15 - Tag cloud for question 3.2 42

Figure 16 - Question 3.3 summary: can a federal service assume the development and management of a new data exchange platform? 43

Figure 17- Tag cloud for question 3.3 45

Figure 18 - Question 4.1 summary: is it relevant for public managers to endorse the role of key regulators in data governance? 47

Figure 19- Tag cloud for question 4.1 48

Figure 20 – Question 4.2 summary: can private actors help adapt and maintain the fraud detection capacities of administrations? 49

Figure 21- Tag cloud for question 4.2 50

Figure 22 - Question 4.3 summary: do these solutions allow for an understandable data governance for all data protection actors? 50

Figure 23 - Tag cloud for question 4.3 52

Figure 24 – Question 4.4 summary: would better communication about new technologies lead to a better understanding and acceptance? 53

Figure 25 - Tag cloud for question 4.4 54

Figure 26 - Question 5.1 summary: can the proposed solutions improve the explainability of AI based decisions? 56

Figure 27 - Tag cloud for question 5.1 57

Figure 28 – Question 5.2 summary: is the development and implementation of explainable tools is within the reach of the different actors? 58

Figure 29 - Tag cloud for question 5.2 59

Figure 30 - Tag cloud for question 5.3 61

Figure 31 - Question 6.1 summary: can these solutions provide a clear and understandable response to DPOs' challenges? 63

Figure 32 - Tag cloud for question 6.1 64

Figure 33 – Question 6.2 summary: can these solutions provide a sustainable response to privacy actors' challenges? 65

Figure 34 - Tag cloud for question 6.2 66

Figure 35 - Question 6.3 summary: can we implement these new approaches to law development? 66

Figure 36 - Tag cloud for question 6.3 68

Table 1 - Anticipated tension points 11

Table 2 - Correspondence between the 6-step model, the survey dimensions, and the evaluation criteria 13

Table 3 - Survey tasks 14

Table 4 – Survey participants 15

LIST OF ACRONYMS

AI: Artificial intelligence

BCT: Blockchain technology

BOSA: Federal Public Service Policy and Support

CSI: Comité de Sécurité de l'information

DIGI4FED: Digital (R)evolution in Belgian Federal Government: An Open Governance Ecosystem for Big Data, Artificial Intelligence, and Blockchain.

DPA: Data protection authority

DLT: Distributed ledger technology

DPO: Data protection officer

EBSI: European Blockchain Services Infrastructure

ESSIF: European Self Sovereign Identity Framework

EU HLEG: European Union high level expert group

FPS: Federal Public Service

FRM: Final reachability matrix

GDPR: General Data Protection Regulation

ISM: Interpretive structural modelling

IT: Information Technology

PKI: Public key infrastructure

OGD: Open government data

WP: Work package

1. INTRODUCTION

The present deliverable is part of the first work package (WP1). Its objectives are threefold. First, the aim of this deliverable is to present an activity report for the testing phase of the living lab process which was conducted with the help of a Delphi survey. This survey was implemented between the 24th of February and the 21st of March, and it obtained the participation of a total of 36 stakeholders from key public and private organizations involved in the fight against fraud. It followed the methods and design outlined in the deliverable 3.3.

The second objective of this deliverable is to report on the results of our analysis of the collected data. The data was analyzed in two different ways. On the one hand, short summary of the results was produced for each question with the help of simple descriptive statistics. On the other hand, we also implemented a qualitative analysis of participants' answers for each question. Taking stock of participants' arguments is critical to understand stakeholders' positions with regard to our proposed governance model. These will provide the needed insights to refine the first version of our governance model for the integration of new technologies (such as AI and BCT) in Belgian federal public policies

Finally, the third objective of this deliverable is to test the validity of our design artefact presented in D3.3. (a governance model for the use of new digital technologies in the fight against fraud in the social security and taxation domain). Taking stock of the analysis results, we propose to assess various key dimensions of our proposed governance model. For that purpose, we used eight evaluation criteria that we previously identified through a literature review of the relevant design science research literature as well as the public administration and public policy evaluation literatures

The design of the deliverable is as follows. In section 2 specify the methods as well as the design of our survey. We also present how it was implemented, and with which participants. In section 3, we present the results of our analysis of the collected data. Participants' answers were analysed using both simple descriptive statistics for participants' answers to each question a qualitative analysis of participants' supplementary answers to these questions. The analysis of each questionnaire question is presented separately and according to the seven main questionnaire sections. The fourth section of this deliverable elaborates on the assessment of our design artefact according to the survey results and the evaluation criteria that were selected in D3.3. More specifically we rely on quantitative benchmarks and a qualitative analysis of the collected data to assess our model based on a predetermined set of eight evaluation criteria. We conclude this deliverable with a summary of the key results of the survey.

2. THE DELPHI SURVEY

This section presents the methods as well as the design of our Delphi survey. We also report on how the survey was conducted, providing details on the various steps that were undergone, the survey participants, and the obtained participation rates.

2.1. THE DELPHI METHOD

NOTE: This section is drawn from D.3.3 (Design artefact and evaluation criteria for testing) which presents the Delphi method and its added value in the framework of the DIGI4FED project.

The Delphi method is "a social research technique whose aim is to obtain a reliable group opinion using a group of experts. It is a method of structuring communication between a group of people who can provide valuable contributions in order to resolve a complex problem" (Landeta, 2006, p. 468). Initially developed and used as a forecasting tool, the Delphi method is the oldest and most widely known of the so-called expert methods (Brady, 2015; Landeta, 2006; Linstone & Turoff, 1975). This technique relies on a multi-round survey process to obtain positions regarding a topic of interest from a panel of experts in a given field. By eliciting such positions, the researchers try to determine the level of consensus or dissensus among experts regarding the investigated topic.

Although there are no strict guidelines, Delphi surveys are generally designed with two survey rounds (Shariff, 2015; Sharkey & Sharples, 2001) and can go up to six rounds (Skulmoski et al., 2007). The number of rounds is usually determined in an iterative manner, depending on the objectives of the study. If the goal is to establish consensus among experts, then three or more rounds may be needed. However, "if the goal is to understand nuances (a goal in qualitative research)", then two rounds might be sufficient uncover sufficient information or reach theoretical saturation (Skulmoski et al., 2007, p. 11). One round can also prove sufficient if the collected data is sufficiently rich. Usually, the first round may use an open-ended format to collect qualitative comments from respondents regarding the issue at stake. Data collected via interviews or focus groups can be used to inform the first round of the survey (Hasson et al., 2000). In between each round, researchers analyze and summarize participants' answers. The obtained results are then fed back to participants through a process of controlled feedback. Summarized responses serve as the groundwork on which the questions of the following rounds of the survey are based. Such a process can be "repeated until consensus is reached or until the number of returns for each round decreases" (Hasson et al., 2000, p. 1010). Participants are not physcally brought together during the process. This facilitates the feeding back of opinions in a non-adversarial manner and reduces the risk of hierarchical bias among panel of participants. In turn, this also promotes participants' mutual understanding and learning about the groups' collective opinion.

The Delphi method is a flexible and pragmatic approach that can be used to answer many research questions with both qualitative and quantitative data sources. Although it is often used in conjunction with some quantitative techniques, many scholars rely on qualitative methods to interpret and analyze the collected data (Brady, 2015; Skulmoski et al., 2007). Indeed, the Delphi method lends itself well to interpretivist approaches by which researchers are "interested in how the social world is interpreted, understood and experienced" (Skulmoski et al., 2007, p. 9). It provides a structured process to rigorously capture rich and detailed qualitative data that allow qualitative researchers to

interpret an object of study in terms of the meaning that respondents place onto them. The thematic analysis (Paillé & Muchielli, 2021; Strauss & Corbin, 1998; Miles & Huberman, 1994) is generally recommended for qualitative Delphi data analysis (Brady, 2015; Linstone & Turoff, 1975).

In the past decades, the Delphi method – that initially centered on the collection of scientific and technical expertise – progressively evolved to integrate a wider pool of participants such as practitioners and individuals with lay expertise on the investigated topic. Nowadays, the panel of participants is no longer necessarily exclusively composed of experts. Depending on the investigated topic, the panel can be made up of all individuals that are deemed relevant either due to their specific competences, their involvement, or their concrete experience (Brady, 2015; Skulmoski et al., 2007; Alder & Ziglio, 1996; Linstone & Turoff, 1975). The aim of the method thus becomes the mobilization of a field expertise via the collection of the multiple perceptions and representations that participants have of a situation. This method thus provides a very complete source of information on the issue at hand while allowing and a first approach to contradictory debate thanks to its multi-round approach. Furthermore, by appealing to respondents' concrete experiences, this approach tends to generate a greater investment and involvement among the associated actors. So far, the Delphi method has been widely used in the field of health sciences, but it has also been successfully implemented in social sciences and information technology (Brady, 2015; Landeta, 2006; Muckherjee et al., 2005; Hasson et al., 2000). The Delphi method is also regularly used for public policy analysis and evaluation. Indeed, the Delphi method allows to apprehend the studied policy sector in all its complexity, and thus provides policy makers with a better understanding of policy design and implementation (Brady, 2015; Alder & Ziglio, 1996; Linstone & Turoff, 1975). Furthermore, by minimizing hierarchical relationships in the communication process, the Delphi method "promotes intersubjective understanding between the decentralized units and with the centralized management" (Fallon, 2018). This can encourage innovation with the emergence of new forms of collaborative governance and knowledge sharing.

The Delphi method provides many advantages that tie particularly well with the objectives of the testing phase of the living lab process that is being implemented as part of the DIGI4FED project:

- First, this method allows to collect a wide variety of opinions by facilitating the expression of a diversity of points of view and experiences. This makes it possible to account for a given problem in all its complexity, by bringing out its multiple constitutive facets. This aspect will be critical to ensure the most comprehensive assessment of our design artifact. It is on that basis that we aim to provide a POC governance model and policy recommendations that account for the diversity of stakeholders' perspectives.
- Second, the Delphi method provides a comprehensive source of information that can serve to initiate debates on a solid and reliable base. As such, Delphi studies are often geared towards informing policy, practice, or decision-making (Brady, 2015; Alder & Ziglio, 1996) because this method can lead to the creation of a consensus on the recommendations, opinions, or modes of action that may emerge from the multiple rounds of the survey. This aspect is particularly relevant in the case of the DIGI4FED project. Indeed, survey participants' reactions to our design artefact will be critical in the development of a POC governance model that reflects a certain degree of consensus among stakeholders. In addition, the conclusions brought by the survey should contribute to the production of policy recommendations to the Belgian federal authorities that may ideally carry a high level of social acceptability.

- Third, Delphi surveys allow participants to express their views on future scenarios that are, in their eyes, both possible and desirable. Such a process can result in high levels of personal investment, with participants taking ownership of the debates and their conclusions. Additionally, Delphi surveys can prompt a learning effect among participants about the issue in question (e.g., Van Dijk, 1990; Schneider, 1971). These elements authorize and encourage a wider dissemination of the debate to the public sphere, thus facilitating the transition from collective reflection to joint action. In the DIGI4FED project, the testing phase of the living lab process aims to elicit stakeholders' reactions to a proposed model for the future of digital governance regarding the fight against tax fraud and social security infringements. In that perspective, it is key to reach high levels of investment and involvement among stakeholders during that critical step. Although the goal of DIGI4FED is not necessarily to generate joint action among the public, the project strives to contribute to the public debate about the possible and desirable futures of digital governance.

2.2. DESIGNING AND CONDUCTING THE SURVEY

The goal of the present survey is to examine various possible *tension points* (Plesch et al., 2013; Sharma & Yang, 2015) in the proposed governance model. In other words, this survey will test several key dimensions of the design artefact that are susceptible to produce *tensions*, or *frictions*, due to the design characteristics of the model and its possible socio-political implications.

As presented in D3.3, five main expected benefits of our proposed model can be put to the fore: 1) The OGD platform should help fostering trust among prosumers, and thus improves the overall endorsement of the system by its users; 2) The proposed design artefact would probably improve the GDPR compliance of new digital technologies in the fight against fraud and facilitate the compatibility of national legislations in relation to the digital framework; 3) The proposed OGD platform should also address the concerns regarding public sector's current dependence on external IT providers while preserving its resources; 4) The proposed design artefact should allow for the use of predictive probabilistic applications of AI without compromising on transparency regarding how this technology is used for decisions; 5) The OGD platform should contribute to the creation of common socio-technical standards and to a greater interoperability among the platform stakeholders at the national and at the EU level.

However, as presented in the following table, each of these benefits also comes with possible shortcomings that might hinder the ability of the model to reach is expected benefits.

Table 1 - Anticipated tension points

Dimensions	Anticipated tension points (and examples)
1. Trust among prosumers and endorsement of the system	Uncertainties regarding the technical maturity of the proposed design solutions. For instance, how close are we from an eventual testing or a pilot stage for this platform?
	Uncertainties regarding our technical readiness to the proposed design solutions. For instance, does BOSA actually hold the adequate technical skills that would be required for the large-scale distribution of digital wallets and deployment of this decentralized platform?

	Uncertainties regarding our socio-political readiness to the proposed design solutions. For instance, to what extent can we expect some resistance to the proposed solutions within the administration? Will governments be able to reach a political consensus regarding the adoption of such a platform and how much time would policy development take?
2. GDPR compliance and compatibility of national legislations	Uncertainties regarding the actual compliance of the proposed design solutions with GDPR requirements. For instance, the assessment regarding the GDPR compliance of EBSI solutions is still pending at the EU level.
	Uncertainties regarding the compatibility of national legislations in relation to the digital framework. For instance, and, although a regulatory sandbox approach might help in developing an adapted regulatory framework, there are still many unknowns regarding the design and methodology of experimental law-making.
3. Public sector's resources and dependence on external IT providers	Uncertainties regarding the predominant role allocated to some specific administrations. For instance, does BOSA possesses the needed expertise and resources to carry such a central role in the development of the platform? Would creating a new dedicated organization in charge of such developments be less adapted for this purpose?
	Uncertainties regarding our ability to allocate sufficient resources to implement the proposed design solutions. For instance, which resources will be allocated to BOSA to spearhead the development and management of this new system?
	Uncertainties regarding the curation and sharing of data with non-public actors? For instance, what data should be allowed for sharing with private actors so that they can develop better predictive technologies without identifying data issuers? Who should oversee the curation of the data used by these actors?
4. Predictive AI and transparency	Uncertainties regarding the technical maturity of XAI solutions. Further testing is still needed to ensure the technical reliability and effectiveness of (X)AI solutions using BCT.
	Uncertainties regarding the appropriateness of the proposed design solutions. For instance, is the proposed system appropriate with regard to existing operational processes in in the fight against fraud? Would it interfere with existing legislative rules in the current framework?
5. Socio-technical standards and interoperability among the platform stakeholders	Uncertainties regarding the involvement of various actors in the development of the proposed design solutions. For instance, which actors will assist BOSA in the development of the EBSI compliant platform? Shouldn't we involve all the potentially interested parties to agree on common standards?
	Uncertainties regarding the acceptance of new socio-technical standards by potential users. For instance, how likely are we to encounter resistance to these new standards due to digital culture differences and digital divide?

In this survey, we propose to assess such tension points taking stock of the evaluation criteria that were selected in previous a step of the project (see D3.3). Taking into consideration these tension points as well as the structure of our proposed model, the present round of the Delphi survey questionnaire was constructed around six key dimensions: 1) Fostering citizen trust; 2) Promoting coordination and interoperability between administrations; 3) Limiting public actors' dependance towards private actors; 4) Values and data governance; 5) Improving the explainability of the analysis

process; 6) Ensuring the legal compliance of the system. The following table presents the correspondence between the 6-step model used to construct our design artefact, the survey dimensions, and the evaluation criteria.

Table 2 - Correspondence between the 6-step model, the survey dimensions, and the evaluation criteria

Steps of the proposed model	Survey dimensions	Evaluation criteria
Contingencies	A. Fostering citizen trust	Overall efficacy; Overall suitability
	B. Promoting coordination and interoperability between administrations	Overall suitability; Overall efficacy; Feasibility
Data prosumers	C. Limiting public actors' dependance towards private actors	Overall efficacy; Overall suitability; Feasibility
Data governance goals	D. Values and data governance	Overall suitability; Sustainability; Overall simplicity; Cognitive aspects
Design values		
Governance of	E. Improving the explainability of the analysis process	Overall efficacy; Feasibility; Sustainability
Governance by	F. Ensuring the legal compliance of the system	Feasibility; Overall simplicity; Sustainability

The survey questions were framed so that respondents could position themselves regarding propositions pertaining to each of the survey dimensions. Some questions were formulated in a closed-ended way, thus asking participants to what extent they agreed, partially agreed, or disagreed regarding specific statements. Participants were also invited to develop their answers and specify why they selected a specific proposition. Some other questions were formulated in a deliberately broad and open-ended fashion so to encourage participants to develop their arguments. We made sure to specify that there are no right or wrong answers to the survey questions. Participants' responses should be grounded on their concrete experience and knowledge on the matter at hand.

The evaluation criteria loosely guided the construction of our questions for each survey dimension. These criteria link with the anticipated tension points because they take stock of the existing literature for model evaluation and are relevant to the potential shortcomings that our team or researchers identified regarding the proposed design artefact (D3.3).

On a practical level, the Delphi survey was organized online with the help of the SPIDEL software. SPIDEL[1] is a new online qualitative survey tool developed in house by the SPIRAL research center at

[1] http://spidel.be/

the ULiège. This tool was specifically developed for use in Delphi surveys. After gathering all the e-mail addresses, names and occupation of our panel of experts, we sent an invitation e-mail containing a link to the online survey. After activation, the questionnaire remained available for over three weeks. During that period, we sent three reminder emails to the experts who did not react to our inquiry. The following table synthetizes the key steps that were undertaken for implementing the survey.

Table 3 - Survey tasks

Date	Tasks
24/02/2022	Activating the online survey questionnaire and sending the invitation emails for the first round
08/03/2022	Sending reminder emails 1
14/03/2022	Sending reminder emails 2
17/03/2022	Sending reminder emails 3
21/03/2022	Deactivating the online survey questionnaire
From 21/03/2022 onwards	Analyzing participant's answers
Approx. 05/05/2022	Sending feedback of the survey results to participants

The survey questionnaires were issued in French, Dutch, and English versions. The Dutch version was translated from French by a team of linguists while the English version was translated from French by the researchers themselves.

No second survey round was planned. However, after analyzing and synthetizing panelists' answers, the obtained results will then be fed back to participants a few weeks after the end of the survey.

2.3. SURVEY PARTICIPANTS

The sample of experts that we invited to participate in the survey was constructed with a purposive sampling approach. The objective was not to obtain a generalizable sample, but to gain input from a "sample of individuals with specific expertise on a topic" (Brady, 2015, p. 2). As a result, the obtained sample was relatively heterogeneous as it comprised various categories of stakeholders who are invested in the integration of new IT tools in the fight against tax fraud and social security infringements in Belgium. In total, our sample comprised a total of 108 stakeholders. Those included:

- Participants to the interviews that were conducted during the exploration phase of the living lab
- Participants to the scenario workshops and solution-oriented workshops

- The follow-up committee members
- People that were recommended to us by the follow-up committee members

In other words, we decided to include all the stakeholders who already participated to the previous steps of the research. These stakeholders were already selected because they are either: 1) directly involved in the use of data (for instance, the CTIF); 2) impacted or have an impact on the use of data in the public sector (e.g., Crossroad Bank for social Security); 3) affected in one way or another by the policies (Banks, Startups, Tech companies, etc.); 4) academics chosen specifically based on their research area.

A total of 108 stakeholders were invited to complete the questionnaire. Among those, 36 participated to the study. This brings our response rate at 33.3 %. As presented in the following table, the stakeholders who participated in the survey originate from various fields of expertise and practice.

Table 4 – Survey participants

Field of expertise / practice	Number of participants
Finances	7
Justice	1
Social security	9
Private sector	7
Federal administration	4
Regional administration	3
European Union	1
Mutuality	1
Union	1
Not-for-profit organization	1
Research	1

3. ANALYSIS OF THE COLLECTED DATA

This section presents the results of an analysis of the collected data. Participants' answers were analysed in two different ways. On the one hand we present a short summary based on simple descriptive statistics for participants' answers to each question. More specifically, we highlight what percentage of participants agreed, partially agreed, or disagreed with our question statements. On the other hand, we also present the results of a qualitative analysis of participants' supplementary answers to these questions. Indeed, the questions were framed so that participants could also develop their answers and specify why they selected a specific proposition. Taking stock of participants' arguments is thus critical to understand their positions with regard to our proposed governance

model. Ultimately, a careful examination of these answers should help us fine-tune and/or reframe the next iteration of our governance model.

3.1. SECTION 1 - FOSTERING CITIZEN TRUST

The first section of the Delphi survey aimed at bringing some possible answers to the lack of citizen trust regarding the use of their personal data by public authorities. Based on the results of the previous steps of the DIGI4FED research project, a series of solutions were presented to the participants. The first consists in improving citizens' ability to control and manage their personal data while the second consists in favoring a decentralized approach to data management that promotes transparency and protection of personal data. The following text box presents the short background piece that was presented to the survey participants:

According to interviews and workshops, **the lack of citizen trust regarding the use of their personal data by public authorities** is a central issue in a context where administrations are using new technologies, such as AI. Some citizens are distrustful of the public authorities that use their data. This distrust is further accentuated by a lack of transparency regarding the (re)use of their personal data (in case of non-compliance with the 'only once' principle, for example). In this context, the ability of citizens to retain a certain degree of control over their personal data is often put forward as a factor that might help in fostering citizen trust.

The governance model could therefore ensure that citizens' trust is enhanced by:

- **Improving citizens' ability to control and manage their personal data**. One solution could be the widespread implementation of a digital wallet system for citizens. These digital wallets would give individuals the ability to control and manage public and private actors' access to their personal data. Such systems, which are often based on the principle of self-sovereign identity, are attracting some interest from public authorities. However, there is no strategic consultation between the different levels of government (federal, regional, and local) at this stage.
- **Favoring a decentralized approach to data management that promotes transparency and protection of personal data**. One possibility could be the implementation of a decentralized platform for data exchange between administrations. This platform could also take inspiration from the Crossroads Bank for Social Security (CBSS) model. Indeed, this system already respects a certain number of good practices that make it possible to meet the requirements in terms of transparency and protection of personal data. This approach could help avoiding an excessive centralization of data.

QUESTION 1.1

The first question of section 1 is as follows: Do you think that such solutions can provide an effective response to the lack of trust among citizens? Could you specify why? Possible answers are: Yes; Partly; No; No opinion.

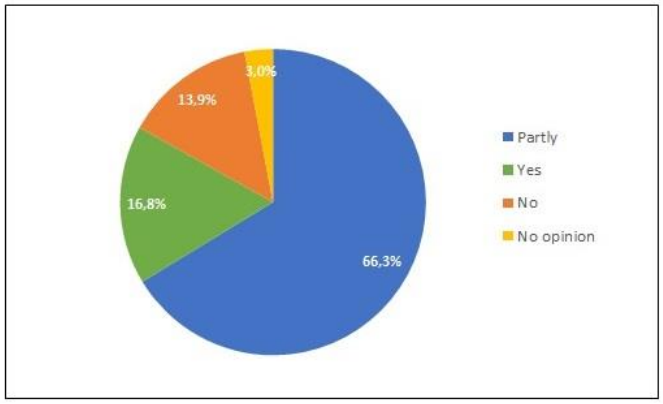
Short summary

A total of 36 participants answered this question. Overall, 17 % of participants agreed that the proposed solutions can provide an effective response to the lack of trust among citizens. 67 % of participants considered these solutions as only partially effective. 14 % did not consider the proposed solution as effective enough and 3 % had no opinion. The following figure synthetizes participants' answers to question 1.1.

Figure 1 – Question 1.1 summary: do these solutions provide an effective response to the lack of citizen trust?

36 answers

e=Partly	24	67 %	
o=Yes	6	17 %	
n=No	5	14 %	
p=No opinion	1	3 %	



Qualitative analysis

In addition to these numbers, a thematic analysis of participants' supplementary answers allowed us to identify five key topics of discussion. The first main topic voiced by participants was a debate over the potential benefits of decentralization or centralization of data management. According to several participants, decentralisation appears as a good solution because it improves security: "The decentralization of the data gives a certain level of security" (social security). Others mention that decentralization can also offer more transparency over the use made of personal data: "for more transparency over the use made of personal data within a government, a decentralized approach to data management with the appropriate governance seems an appropriate solution" (regional administration).

Although some participants voiced their agreement, many expressed some criticism regarding a decentralized approach to data management. Indeed, these stakeholders expressed their lack of confidence in this technical solution: "But then one must still have confidence in the proper functioning of the decentralized platform" (Finances). They also expressed their concern that a decentralized solution might create too much "overhead for citizens" (Not-for-profit organization) and that it may appear to abstract to generate trust among citizens: "Concerning decentralization, I think it is a very relevant tool, but it will not be a tool for improving citizen trust. These concepts are far too abstract for the average citizen" (Social security). Some participants also advocated for a combination of a centralized and a decentralized approach of data management. They argued that, although decentralization provides some level of security, "metadata must be kept centralized" (social security).

The second main topic voiced by participants is citizens' personal data management. Many participants saw in a positive light the potential gains in transparency brought by digital wallet solutions regarding the use of citizens' personal data by public authorities. Indeed, some participants praised digital wallets' potential for fostering citizens' trust: "A higher degree of transparency enables citizens to view and check the data on which decision-making is based, which has a positive effect on trust and perhaps even on the intrinsic desire to do things properly (compliance). It also promotes efficiency, which is positively valued by citizens" (Private sector). Other participants emphasized that, besides transparency, it is also citizens' enhanced ability to control who accesses their data that is a

key factor for generating trust: “A combination of both approaches seems optimal: for more control over the sharing of personal data with companies in particular, a digital wallet seems an appropriate solution, for more transparency over the use made of personal data within a government, a decentralized approach to data management with the appropriate governance seems an appropriate solution” (Regional administration). Similarly, “giving citizens the rights to think about and manage the access to their own personal data is surely a good thing for trust and also convenience improvements for them” (Scholar).

A few participants consider that the model should go one step further by providing full transparency to citizens as well as the ability to fully control and manage their personal data: “Improving the citizen's/company's ability to control and manage their data is a prerequisite. But it is not enough. The citizen/company must have full transparency, i.e., know exactly how and why his/her data is used. Furthermore, he/she must be free to accept or refuse this data processing, and this in an easy way (not after having to read 100 pages that are not easily understandable).” (Private Sector).

On the opposite, a considerable number of participants pointed the limits of digital wallets solutions. Some argued that digital wallets would not necessarily help fostering trust among citizens if citizens are not convinced with the good intentions of those who are issuing and managing these wallets: “The citizen must be convinced that these tools guarantee the correct processing of this data. How can they be convinced that the digital portfolios are reliable and processed as theoretically intended? The citizen must be convinced of the transparency and honesty of the model” (Social Security). Other participants stressed that citizens’ ability to control their data should remain somewhat limited, especially when it comes to granting access to some of their data to public authorities: “there are surely a lot of government linkages to the data that would be non-optional, since many government agencies definitely need more access to citizen data then others” (Scholar). Similarly: “It is legitimate to want to make sure that the citizen can better manage and control his personal data. However, the citizen should not necessarily have the choice to share or not his data with the administrations (e.g.: e-health platform, it is not up to the citizen to determine if doctors should be informed or not of medical history). When outside of this relationship with public authorities, it is positive to give citizens the ability to better manage their data” (Social security).

The third main topic voiced by participants was citizens’ trust. A significant number of participants stressed that the proposed design solutions would probably not greatly improve citizens’ trust regarding the use of their personal data by public authorities because the main underlying issue remains citizens’ mistrust of public authorities in general: “It is not so much the tool that has been put in place as the people who manage the tool that scares and loses the trust of the citizen. The citizen is ready to reveal personal data for a TV game show but will hesitate for the state because he is afraid of what the latter could do with the information” (Private sector). Many of these participants further stress that there is a contradiction between citizens’ lack of consequentialism when sharing their personal data with private companies and their apparent mistrust of public authorities using their personal data: “Citizens who do not 'trust' are the first, via the applications they use on their smartphone or computer, to 'entrust' their data to actors often outside Europe” (Regional administration).

The fourth topic brought by stakeholders was the importance of communication with citizens. Some participants stressed that formulating technical solutions and developing new tools (such as digital

wallets) might not suffice to foster trust as long as a good communication with citizens is lacking: "More clarification is needed for citizens than this. There are currently concrete plans to roll out a digital portfolio at the federal level by 2023. This instrument is currently mainly aimed at storing documents and data in a digital manner and possibly making them available to the government. However, a digital portfolio does not immediately give citizens more explanation of what their data will be used for. It is precisely this aspect that provides peace of mind and confidence for the citizen" […] "Good communication with the citizens could possibly provide many solutions" (Social Security).

The fifth main topic was the level of IT related skills among citizens. A limited number of participants were concerned that the proposed solutions would prove too complex or not user friendly enough "to include as many people as possible" (Scholar). According to these participants, the risk is that the proposed solutions (decentralization and digital wallets) would exclude many citizens, including those who are already affected by the digital divide. The digital divide issue was further addressed by participants in their answers to the next question (question 1.2).

The following figure presents a tag cloud that synthetizes the themes that were identified during the qualitative analysis of question 1.1.

Figure 2 - Tag cloud for question 1.1

QUESTION 1.2

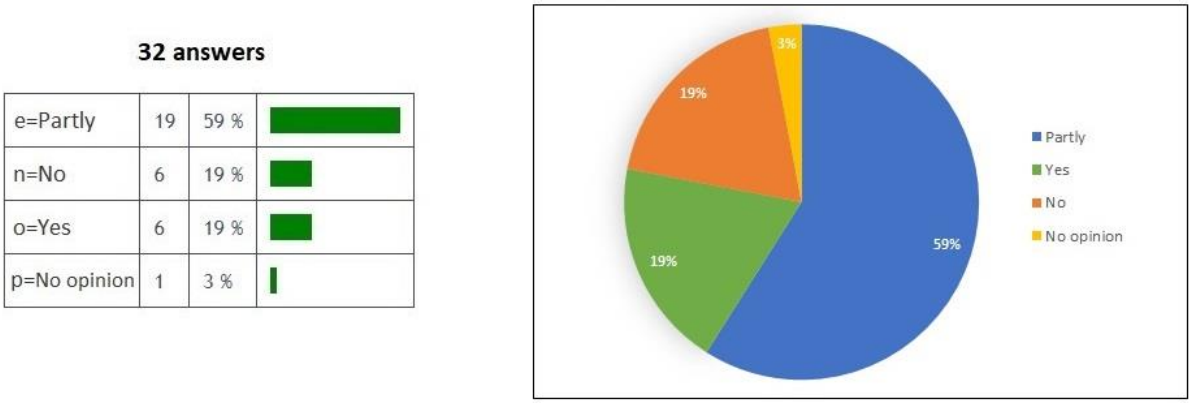
The second question of section 1 is as follows: Do you think that the generalization of a digital wallet system could be an adequate solution to a lack of citizen trust? Could you specify why? Possible answers are: Yes; Partly; No; No opinion.

Short summary

A total of 32 participants answered this question. Overall, 19 % of participants agreed that digital wallets can provide an adequate response to the lack of trust among citizens. 59 % of participants

considered digital wallets as a solution that is only partially adequate while 14 % did not consider it adequate. 3 % had no opinion. The following figure synthetizes participants' answers to question 1.2.

Figure 3 – Question 1.2 summary: are digital wallets an adequate solution to a lack of citizen trust?



Qualitative analysis

In addition to these numbers, a thematic analysis of participants' supplementary answers allowed us to identify five key topics of discussion. The first main topic voiced by participants was citizens' personal data management. As for the previous question, many participants tended to approve the potential gains in control and transparency that can be brought by digital wallet solutions: "the system of digital portfolios is an element that, in part, in combination with other applications and communications can contribute to a better bond of trust" (Social security). Similarly, "a citizen must be able to check data and be offered an easy process to correct inaccuracies and complete incomplete data" (Private sector); "the positive effect lies in the empowerment that one gives to the citizens who consider this important" (Social security). However, and as previously mentioned, several participants also mentioned that digital wallets solutions should go one step further by providing full transparency to citizens as well as the ability to fully control and manage their personal data. To these participants, digital wallets appear "essential but not sufficient. It is necessary to allow the possibility of participating in the management and use of one's data, especially medical data, and to modify it without having to go through tedious and costly appeal procedures if necessary" (Social Security).

A significant number of participants also pointed out the limits of digital wallet solutions. Again, some argued that digital wallets would not necessarily help fostering trust among citizens if citizens are not convinced with the good intentions of those who are issuing and managing these wallets: "This solution is not a magic tool to gain trust and can have the opposite effect (feeling that the government is collecting a lot of data on its citizens)" (Not-for-profit organization). Other participants stressed that citizens' ability to control their data should remain somewhat limited, especially when it comes to granting access to their data to public authorities: "However, one must be careful that the citizen does not have to give his permission to the government every time and everywhere to be able to use these data: if it has been decided democratically that the government can use certain data in the framework of its policy, functioning or service provision, then this must be possible without having to ask explicit permission every time" (Regional Administration).

The second main topic mentioned by participants was citizens' trust. As for the previous question, a significant number of participants stressed that digital wallet solutions would probably not greatly improve citizens' trust regarding the use of their personal data by public authorities because the main underlying issue remains citizens' mistrust of public authorities in general: "For a part of the citizens, such digital wallets will give the impression that the government wants to gain more control over them instead of the other way around. And if it is not the government, then it is the device and operating system providers (Apple, Google, Microsoft) on which such digital wallets will be used, to which citizens will have to put their trust even more." (Federal Administration). Similarly, "A part of the population will just be more suspicious by a system of digital wallets, even if they would be 'voluntary', this would still eventually become a form of obligation" (Federal Administration). In the end, some argue that "the main lever for restoring trust in government remains the proper service delivery by its departments" (Social Security).

The third main topic voiced by participants was the importance of communication with citizens. Again, a significant number of participants stressed that digital wallets might not suffice to foster trust if they are not accompanied by effective communication efforts from public authorities: "Good and clear communication remains the most important element for creating a bond of trust in the first place. However, the system of digital portfolios is an element that, in part, in combination with other applications and communications can contribute to a better relationship of trust" (Social security). Similarly, "the State and its administrations suffer from an ancestral and very dusty image where communication goes only in one direction except for taxes .... a big work of communication should be set up in order to change the vision of the citizens on the State, its functioning... and that they can feel that actions are really undertaken for their well-being" (Justice). In other words, "the benefit for the citizen in terms of services must be made obvious" (Not-for-profit organization) and communication efforts might help on this aspect.

The fourth main topic was the issue of digital divide and the level of IT related skills among citizens. A significant number of participants were concerned that digital wallet solutions would become a hinderance for some citizens and small businesses due to their complexity and their lack of user friendliness: "we assume that the citizen or the company will know how to use it ... we are far from the account, see the little use of the ebox. the technique can't do the job" (Regional administration). Similarly, "To this day, there are those who do not yet have a bank card. They are still far away from digital wallets. The generalization of such a system will take years (maybe decades)" (Finances). According to those participants, the risk is to "lose sight of the people who are not "on board" with digitalization" (Social security). However, one solution to remedy this issue would be through adequate communication and education: "This could help, but if it is accompanied by information and EDUCATION of the citizens to this initiative" (Regional administration).

The fifth main topic brought by respondents concerns the possible technical issues with regard to digital wallet solutions. One of such potential issues is security as some argue that the multiplication of wallets could lead to security risks: "Citizens don't want 'wallets'... they want to be able to manage their data in a secure way. The importance must be given to an 'authentic' source and the interoperability of the blocks of information between interfaces chosen by the citizens. for example, via its bank app, or other. The multitude of wallets could lead to security risks..." (Federal

Administration). In other words, it is important that “processes around data governance, security personal data, data retention etc. can be guaranteed by government” (Private sector).

The following figure presents a tag cloud that synthetizes the themes that were identified during the qualitative analysis of question 1.2.

Figure 4 - Tag cloud for question 1.2

QUESTION 1.3

The third question of section 1 is as follows: Do you think that a decentralized data management could be an appropriate response to a lack of citizen trust? Could you specify why? Possible answers are: Yes; Partly; No; No opinion.

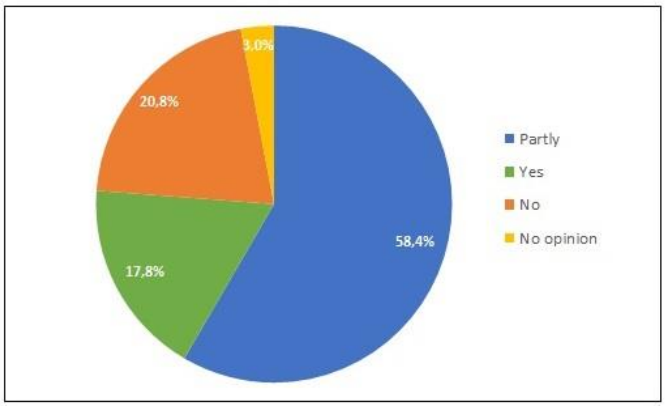
Short summary

A total of 34 participants answered this question. Overall, 18 % of participants agreed that a decentralized data management system could be an appropriate response to a lack of citizen trust. 59 % of participants considered this solution as only partially appropriate while 21 % did not consider it as appropriate. 3 % had no opinion. The following figure synthetizes participants’ answers to question 1.3.

Figure 5 - Question 1.3 summary: is decentralized data management an appropriate response to a lack of citizen trust?

34 answers

e=Partly	20	59 %	
n=No	7	21 %	
o=Yes	6	18 %	
p=No opinion	1	3 %	



Qualitative analysis

In addition to these numbers, a thematic analysis of participants' supplementary answers allowed us to identify three key topics of discussion. As for question 1.1, the first main topic voiced by participants was a debate over the potential benefits of decentralization and centralization of data management. According to a number of participants, decentralization appeared as a good solution. Some argued that decentralization provides greater security because "not all personal data is stored in one place and is combined and used there in the wrong way, or that all this data becomes known if the central data storage is hacked by cybercriminals" (Regional administration). Others further argued that excessive centralization of data can lead to mistrust among citizens: "Decentralization of data provides a certain level of security. Too much centralization creates a feeling of loss of control among citizens, fear that we have a global cadastre of health data" (Social Security). Some participants also argued in favor of the BCSS model as it illustrates some of the advantages of a somewhat decentralized approach to data management: "The CBSS model is definitely recommended" (Private sector). On that regard, some participants also expressed their preference for a hybrid approach to data management with the idea that "Management should be centralized, storage decentralized" (Social security) and that although some degree of decentralization can be introduced, "The unique 'key' must be managed by a reliable manager" (Federal administration).

Despite some arguments in favour of decentralization, many also expressed some criticism towards this approach. Indeed, some stakeholders stated that they were not convinced that decentralization could generate trust among citizens: "Decentralized means that data is distributed to multiple parties. This creates distrust" (Social security); "Decentralization alone will not create trust" (Federal administration). On the opposite, some argued that a centralized approach is more beneficial for citizen trust: "On the contrary, I believe that a centralized approach, but in full transparency and with a sound infrastructure and governance will do good for trust" (Private sector). Others considered decentralization as far too complex and abstract to be a convincing solution for citizens: it is "not visible and too abstract for the citizens. Even if it does in fact contribute to this, the average citizen cannot understand that this action is done for this purpose and does not see the results (not tangible for him)." (Justice). Similarly, "Citizens are presumably not always aware of the implications of

(de)centralized data management" (Social security); "A decentralized approach to data management is more technically complex than a centralized approach" (Regional administration).

Some participants also questioned the relevance of a decentralized approach given that the use case remains unclear to them: "Use case not clear: Blockchain can be useful to make certificates unforgeable for example, but not sure of the added value on a larger scale" (Social security). In addition to the relevance of this approach, others questioned the technological maturity of decentralized solutions, such as blockchain: "Decentralized data storage solutions (especially the Blockchain) raise many questions: 1) What is the added value, knowing that the encryption of data which is secure today may not be secure tomorrow because of the rise of computational capabilities. 2) Maturity of the technology: we have no hindsight" (Social security).

The second key topic voiced by participants was the importance of communication with citizens. Again, some participants stressed that privileging a decentralized approach to data management might not suffice to foster citizen trust without communication efforts from public authorities: "This is not a conclusive solution but rather a means. Again, proper communication of this is vital" (Social security). "For trust, however, one must explain to the citizen what exactly decentralized data management means" (Finances).

The third main topic concerns some stakeholders' general reflections and observations regarding the use of data by public authorities. Some argued that in order to improve trust among citizens, public authorities should consider minimizing their general use of citizen data: "Improved service and a government that helps minimize (not just decentralize) personal data should certainly also be part of any effort to increase trust" (Federal administration). Another observation was the necessity to have a general reflection about the meaning and the quality of data within administrations: "without control of the quality of the data (and their conservation in time), and especially of the meaning we give to them (different semantics according to the professions) ... we risk mixing apples and pears" (Regional administration).

The following figure presents a tag cloud that synthetizes the themes that were identified during the qualitative analysis of question 1.3.

Figure 6- Tag cloud for question 1.3

3.2. SECTION 2 - PROMOTING COORDINATION AND INTEROPERABILITY BETWEEN ADMINISTRATIONS

The second section of the Delphi survey aimed at bringing some possible answers to the lack of interoperability and coordination between administrations. Based on the results of the previous steps of the DIGI4FED research project, a series of possible solutions were presented to the participants. The first consists in the adoption of a data exchange platform that would operate based on common criteria and technical standards while the second consists in the creation of an entity in charge of coordinating, developing, and monitoring digital projects within the administrations. The following text box presents the short background piece that was presented to the survey participants:

Results from the workshops and the interviews suggest that **the lack of interoperability and coordination between administrations** is a central issue faced by administrations using new technologies in the fight against fraud. This dynamic tends to result in a considerable waste of energy and resources when administrations develop similar digital projects separately. In addition, this lack of coordination also makes it difficult for administrations to share data and make their respective databases interoperable.

The governance model could therefore ensure to improve the coordination and interoperability between administrations with:

- **The adoption of a data exchange platform that would operate based on common criteria and technical standards**. The implementation of such a platform would stimulate data interoperability and collaboration between all actors in charge of fighting tax fraud and social security infringements. Under certain conditions, this solution could also facilitate cooperation with European counterparts who have set up an equivalent system.
- **The creation of an entity in charge of coordinating, developing, and monitoring digital projects within the administrations**. One solution could be to empower some existing Federal Public services (FPS), such as the FPS BOSA, or to create a new entity along the lines of the Smals organization, but which would offer its expertise to all FPSs. This new entity would ensure the harmonization of projects and the development of a common strategic vision. It would also be responsible for the development and management of the data exchange platform or the deployment of digital wallets, for example.

QUESTION 2.1

The first question of the second section of the survey is as follows: In your experience, what is the most important barrier to coordination and interoperability between administrations?

Qualitative analysis

A thematic analysis of participants' answers allowed to identify three main categories of answers to this question. First, a significant number of participants mentioned the organisational barriers to coordination and interoperability between administrations. In other words, obstacles that are rooted in the way administrations tend to operate in Belgium. Among these organisational obstacles, a prominent issue is the lack of dialogue and communication between services. Administrations tend to operate in Silos, which makes them unaware of what data is collected and stored in the databases of other administrations: "Fraud information is not always transmitted to other administrations because of a lack of awareness of the interest it may have for these other administrations; The existence of certain relevant data at the disposal of another administration is not known or the interested person does not know where he/she can go to obtain it" (Finances). Administrations are "not thinking in networks" (Regional administration), which makes it difficult to "find appropriate contacts within other government agencies that provide data" (Social security). Because of this lack of contact, civil servants also tend to remain unaware of the projects that are developed in other services: "Lack of contact. Only the top officials may be aware of the projects in other government departments. If the operational departments do not know about the existence of certain information, it may not ask for it to be exchanged either" (Finances).

Similarly, other participants mentioned that the lack of coordination can also result from a misalignment in political and institutional priorities and that this phenomenon can further encourage divergences between administrations over time: "The biggest obstacle to coordination is that government entities at different levels of government now have different political and institutional

priorities that are not always aligned" (Regional administration). "The (political) division between the various federal government departments, as it were, a continued 'compartmentalization' often exacerbated by successive legislatures, that repeatedly shakes up the policy per department." (Social security).

Other participants described a lack of wilfulness to share their data with other administrations: "Some jurisdictions don't want to share their data easily and the process to get it is cumbersome and slow" (Finances). They also observe that administration tend to have "little wilfulness, very risk-averse approaches" (Social security), which denotes a "Lack of long-term strategic vision" with "Ad hoc political decisions based on short-term thinking...." (Federal Administration).

The second main barrier voiced by participants resides the shortcomings associated with the lack of a clear normative and legal framework. On the one hand, a significant number of participants stressed the lack of a comprehensive legislation on data exchange at the national and international level: "The main problem is that there is no legal framework that clearly defines the exchange of data. Each member state interprets certain European rules differently so that it is possible between some member states and not with others. At the national level (I have less experience with this), I think it happens less because it is so cumbersome to get access to the data. Very often it requires sitting down together first between the presidents of the different government departments. I know of a project where we are asking for data from another government department that has been dragging on for a few years. Very often it is legal problems, but technically everything is perfectly possible" (Finances). A similar issue is also present between the different levels of government: some observe a "lack of alignment between laws and regulations at different levels of government (legal interoperability)" (Regional administration). Similarly, other stakeholders mention that the current framework imposes legal barriers that complicate data exchange and processing, especially across different policy sectors: "There is still a lack of transversality with the tax authorities (legal obstacles exist but sometimes these obstacles are also used as excuses not to share information (tax-related information of a company that can be very useful to demonstrate social fraud). Only the legal route then allows tax data to be cross-referenced with tax data" (Social security).

On the other hand, participants also mentioned the lack of common procedural and technical standards that would ease data exchange and interoperability between administrations across policy sectors: "Within the same FPS, there are indeed possibilities of interoperability. On the other hand, for the exchange between FPSs, there is, to my knowledge, no common platform. Protocols between FPSs exist but are sometimes long to set up. An IT platform common to all FPSs would allow access under certain conditions to data from various organizations. The conditions of access can be partly motivated in a document proving the principles of finality, proportionality, such as the Data Access Management or DAM form). It would also be necessary to set up a business and technical documentation allowing transparency and understanding of the existing data in each Administration. This could lead to joint actions in certain areas (fight against fraud, etc.)" (Finances). Similarly, "The biggest barrier to interoperability between government services is the establishment of and adherence to sufficient common technical standards for data exchange and application integration (technical interoperability)" (Regional administration).

The third main barrier voiced by participants resides in the practical and technical difficulties in achieving interoperability. Participants notably mentioned the fragmentation of data across the

various administrations: “The health data is very fragmented between different institutions” (Social security). In addition, datasets are usually “not compatible with each other in their current state” (Social security). In some instances, the existing data is even unstructured and unusable in its current state: “Files of judicial investigations (justice/police) are often still on paper, sometimes only partly digitized and then mainly file bound. Digitization means making one or more CDs of the official reports and conviction documents. Sometimes parts of these are still with the federal public prosecutor's office and other parts with a local public prosecutor's office” […] “paper documents are scanned and together with digitized documents are made accessible. In other words, it is unstructured data. Interoperability would then require that a central e-discovery platform be set up” (Finances).

In addition to the characteristics of the data, the problem also lies in the lack of technical skills and expertise within administrations. According to some participants, there are important disparities between administrations regarding IT expertise. Some administrations still use “legacy and almost obsolete applications” (Regional administration). This “lack of uniformity in IT developments and the discrepancy between their level of development between the different administrations” (Mutuality) can also complicate data exchanges between administrations. Others stress a lack of knowledge about “data semantics” (Federal administration) or, in other words, a lack of data expertise in administrations.

Although most agree that there are barriers to coordination and interoperability between administrations, a limited number of participants argued that coordination and interoperability is currently not an overarching issue: “I don't understand where the idea comes from that there is no interoperability. The FPS BoSa DG DT (the former Fedict) is a service integrator; the platform on which the data flows are exchanged (not stored) is the Federal Service Bus; all services are managed according to EU standards with focus on interoperability and security/protection of privacy (Isa², Oslo², ...)” (Federal administration). Similarly, “I disagree with this view and the 'direction' of your question, which implies that this problem is everywhere and all the time. This is not the case. In Wallonia, it is the raison d'être of the Digital Agency (AdN) to set up and operate a regional strategy for the digital transformation of the territory, which involves all the ecosystems and materializes this 'other governance' that you advocate” (Regional administration).

The following figure presents a tag cloud that synthetizes the themes that were identified during the qualitative analysis of question 2.1.

Figure 7- Tag cloud for question 2.1

QUESTION 2.2

The second question of the second section of the survey is as follows: Do you think that the proposed solutions could help overcome this obstacle? Could you specify why? Possible answers are: Yes; Partly; No; No opinion.

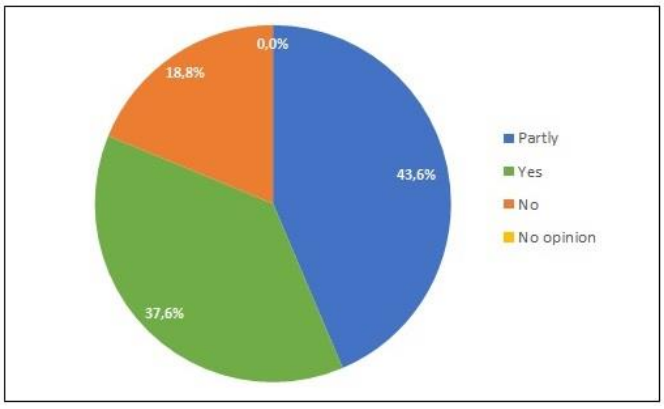
Short summary

A total of 32 participants answered this question. Overall, 38 % of participants agreed that the proposed solutions could help overcoming the lack of coordination and interoperability between administrations. 44 % of participants considered this solution as only partially helpful while 19 % did not consider it helpful. The following figure synthetizes participants' answers to question 2.2.

Figure 8 - Question 2.2 summary: can these solutions help overcome interoperability and coordination issues?

32 answers

e=Partly	14	44 %	
o=Yes	12	38 %	
n=No	6	19 %	
p=No opinion	0	0 %	



Qualitative analysis

In addition to these numbers, a thematic analysis of participants' supplementary answers allowed us to identify three main topics of discussion. Most respondents reacted to the adoption of a shared data exchange platform that would operate based on common criteria and technical standards. In that regard, a first main topic of discussion concerns participants' reactions to the idea of adopting of such a platform. A significant number or respondents reacted positively to this solution: "The platform would be an optimal solution in theory" (Social security); "it is useful to change mentalities and to encourage the sharing of information (to avoid private hunting grounds)" (Social security); "This can be a very good starting point" (Finances). Overall, this solution was often perceived as a good way to achieve a de-compartmentalization of services. Some participants stressed that this solution would be best adopted combination with the second proposed solution (i.e., he creation of an entity in charge of coordinating, developing, and monitoring digital projects within the administrations): "This can certainly be a solution. The newly established one can thus centrally address all kinds of data problems of the different institutions and achieve equal solutions between the different institutions" (Social security).

Although generally favorable, a considerable number of participants also voiced some caveats regarding the adoption of this common data exchange platform. First, regarding the characteristics of the platform, some voiced their preference for a centralized approach regarding the platform governance: "Centralized governance is essential" (Private sector). Others advocated for a combination of centralized and decentralized approaches for data management: "A centralized platform with metadata is needed. Transactional data can remain local. Master data and repositories should also be centralised" (Social Security). Second, participants formulated some precautions and recommendations regarding how data should be treated, shared, and with what purposes on the platform. Some mentioned that the data shared on the platform should preferably have multiple uses: "A platform for data exchange would help if the information supports multiple modes of use. Exchanging information at the individual level has different implications than at the level of (sub)populations" (Social security). Others stressed that the platform should also contribute to the streamlining of data extraction procedures: "Unstructured data only needs to be prepared once (adding, extracting, OCR, entity recognition, ..." (Finances). Third, regarding legal aspects, some participants mentioned that this platform should above all fit within a clear legal framework, and that it will have to comply the existing restrictions in terms of privacy: the platform is not a good solution "if it is limited to providing technical solutions, but above all a clear legal framework and realistic guidelines are needed to guide administrations" (Not-for-profit organization); "Privacy laws will always remain and thus impose the necessary restrictions" (Social security). Fourth, participants also mentioned that, to ensure success, the collective advantages brought by this platform should be clearly advertised to all involved parties: "As with the creation of the Crossroads Bank for Social Security, the common interest, the win-win, needs to be emphasized across all parties (political, administrations). Objective criteria and standards facilitate this understanding" (Social security).

Some respondents were not favourable to the adoption of this shared data exchange platform. Various arguments were put forward. Some considered that the standardisation of data and procedures should receive a greater priority than the creation of a new platform: "Why not standardize work and data" (Private sector). Others are doubtful as to the capabilities of departments to collaborate with other partners on a project involving such a wide array of expertise: "All our data mining projects with external consultancy have failed. Without knowledge of the subject matter

(legislation, how something works in practice, ...) it is impossible to build a working data mining model. It is much better to have dataminers working within the government department. That way they have close contact with the experts and can acquire this knowledge themselves" (Finances). Some other participants argued that such a platform is not needed if it is just to occasionally share some specific data between services: "It must be possible to share specific data on the basis of very concrete needs without them being part of a single platform" (Social security).

The second main topic voiced by some respondents is the existence, within administrations, of systems that they consider close or similar to the proposed solution for a common data exchange platform. In other words, a number of participants argued that such a platform system already exists at least partially at the regional and federal level: "In my view this already exists and is already being fulfilled. (BOSA federally, MAGDA Flanders). But not as it ideally could be, given the obstacles as indicated in point 2a" (Federal administration); "These solutions already exist (ODWB) and it is useless to want to create yet another body..." (Regional administration); "This approach is already largely being followed within the Flemish government: with the MAGDA data-sharing platform, we already have a platform for data exchange that works on the basis of common criteria and technical standards, and with the creation of the Digital Flanders agency, we already have an entity that is increasingly responsible for the coordination, development and follow-up of digital projects within the Flemish government departments" (Regional administration). Participants also pointed to the existence of service integrators at the federal and regional level which serve the purpose of facilitating the sharing of data between administrations: "Yes, BOSA's is optimal and has already proven itself with the entire ecosystem of integrators." (Federal administration).

The third main topic of discussion concerns the need for an entity in charge of coordinating, developing, and monitoring digital projects within the administrations. Many participants agreed that such an entity would be instrumental in ensuring a greater coherence of action and collaboration between parties: "The entity, if it really obtained the means to accomplish its role vis-à-vis the administrations involved, would certainly allow for better uniformity and collaboration between institutions that must accomplish the same objectives" (Social security). Similarly, "The new institution to be set up can thus deal centrally with all kinds of problems relating to data from the different institutions and achieve equal solutions between the different institutions" (Social security). However, some participants stressed that, to be successful, this new entity should make sure to listen and respond to the specific needs of each administration: "but must be able to listen to the entities and respond to the needs of each entity (tailor-made), otherwise individual initiatives will reappear very quickly, and it will lose its strength (cf. BOSA)" (Justice).

A few participants did not agree with the creation of a new entity in charge of coordinating, developing, and monitoring digital projects. They argued that, although some entity should definitely be entrusted with this mission, a completely new entity should not be created: "While the presence of an entity in charge of project coordination/development/monitoring seems useful and necessary, it seems essential to avoid creating an additional entity. The multiplication of actors complicates management. What is needed is a simplification. The less actors there are, the less interoperability problems arise..." (Private sector).

The following figure presents a tag cloud that synthetizes the themes that were identified during the qualitative analysis of question 2.2.

Figure 9 - Tag cloud for question 2.2

QUESTION 2.3

The third question of the second section of the survey is as follows: Do you think that such a data exchange platform between administrations is feasible (legally, organizationally, etc.)? Could you specify why? Possible answers are: Yes; Partly; No; No opinion.

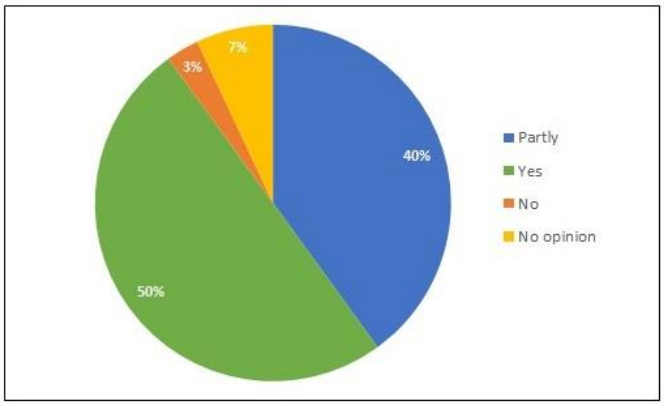
Short summary

Overall, 50 % of participants agreed that a data exchange platform between administrations is a feasible option when addressing the lack of interoperability and coordination between administrations. 40 % of participants considered this solution as only partially feasible while 3 % did not consider it feasible. 7 % had no opinion. The following figure synthetizes participants' answers to question 2.3.

Figure 10- Question 2.3 summary: is a data exchange platform between administrations feasible?

30 answers

o=Yes	15	50 %	
e=Partly	12	40 %	
p=No opinion	2	7 %	
n=No	1	3 %	



Qualitative analysis

In addition to these numbers, a thematic analysis of participants' supplementary answers allowed us to identify three groups of factors that might affect the feasibility of the proposed data exchange platform. Participants were generally positive regarding the feasibility of this design solution.

First, many participants evoked the technical and practical aspects that might affect the feasibility of this platform. As already developed in the previous question, participants mentioned the existence of systems that they already consider close, or similar, to the proposed data exchange platform. Some took the CBSS model as a proof that the creation of such a platform should be possible without any major obstacles: "The creation of the Crossroads Bank for Social Security has proven that this should be possible" (Social security). Others argued that the creation of such a platform is viable as some projects and discussions are already ongoing, including at a transnational level: "This can even be considered beyond the national level, i.e., at the Benelux or EU level in several areas (social posting of workers within the EU or economic, fight against mailbox companies, access to commercial data of companies). Experiences are emerging, and exchanges are taking place to discuss and try to develop a data exchange or even better an access to data directly through a common platform" (Social security). Several participants noted that some existing tools already try to achieve a similar outcome at the regional and federal level. These respondents took as example the service integrators which already serve the purpose of facilitating the sharing of data between administrations at the federal and the regional level: "The existence and growing success of the MAGDA data sharing platform demonstrates that such a platform for data exchange between administrations is possible" (Regional administration); "Some of this already exists, namely the system of service integrators" (Federal administration).

The second group of factors that might affect feasibility concerns the legal framework. Some participants mentioned that such a platform should be feasible from a legal standpoint as long as it fits within a clear legal framework, and that it complies with the existing legal requirements in terms of privacy protection: "Yes, as long as, in order to comply with the different legislation (RGPD, privacy), the access of data to a user (or function) has received the approval of the competent authority in charge of Information Security and Privacy Protection, which must verify that the functional interest

of the user is justified (examination of the purpose, proportionality and security) and must thus guarantee access to data that is adequate and relevant and not excessive in relation to the exercise of its legal missions" (Finances); "Taking into account legal restrictions, it should be possible to build a central platform for data" (Private sector); "From a legal point of view, I think this would be possible. It would be a matter of each administration justifying to the competent entity the reasons for access to this data within the platform. The accesses would be regulated according to the existing or obtained authorizations" (Social security). Some other participants noted that such a platform would have to address the possible legal challenges associated with the need of ensuring the secrecy of ongoing investigations: "There will be significant challenges, though, such as maintaining the secrecy of the investigation, on the other hand, ensuring tax professional secrecy" (Finances).

The third group of factors voiced by participants concerns organizational aspects and the resources of administrations. Some participants argued that the creation and monitoring of such a platform would require considerable resources from the administrations: "This requires that sufficient resources will be allocated to this newly created entity (allocation of cash, knowledge, infrastructure and personnel)" (Social security). However, with an adequate budget, the implementation of such a platform should be possible: "It depends on the budgets that are allocated (technical architecture, human resources, etc.)" (Finances). Other participants mentioned the risks of internal resistance within administrations, as some services will probably try to protect their specificities: "For me, the biggest difficulty will be to avoid baronial fights within the services that will want to keep their particular specificities that are not necessarily indispensable" (Private sector).

The following figure presents a tag cloud that synthetizes the themes that were identified during the qualitative analysis of question 2.3.

Figure 11 - Tag cloud for question 2.3

QUESTION 2.4

The fourth question of the second section of the survey is as follows: What do you think would be the most appropriate organizational choice to ensure the coordination, development, and monitoring of future digital projects? Could this role be played by the FPS BOSA or by a new entity on the model of Smals (not-for-profit organization) as indicated by some actors? Do you see other possibilities?

Qualitative analysis

A thematic analysis allowed to identify three main categories of answers to this question. First a considerable number of participants voiced their preference in favour of a federal administration for handling the coordination, development, and monitoring of future digital projects. Among participants, many argued in favour of BOSA to assume this task: “Given the data, the legal sensitivities, and perceptions, this should be given to an FPS. The mission of BOSA is clear - to serve others. This approach also allows for direct progress since the solutions exist and the legal framework does not require major adaptation” (Federal administration). Similarly, “FPS BOSA is to be preferred. It is one of the reasons why Fedict, now DG Digital Transformation, was once created. It does not make sense to assign this to an external party such as a government non-profit” (Private sector). “If FPS BOSA can act with sufficient autonomy and authority, there is no need to create a new department” (Social security). Some other participants also voiced their preference for a federal administration but without designating BOSA as the most likely candidate: “this body would have an enormous amount of concrete personal data at its disposal. As a result, it seems important to me to assign this to a body that is under full government control” (Social security); “In Flanders, however, this role is increasingly being entrusted to the Digitaal Vlaanderen agency, so it would be useful if this agency were to be given a similar counterpart and discussion partner at federal level” (Regional administration). An inter-federal agency was also proposed as possible solution: “I don't think that bosa can perform this role. It will have to be entrusted to another entity, we could talk about an inter-federal agency (one or more with representatives of the different SPFs concerned)” (Social security).

Second, some participants advocated for a collaboration between private and public actors. The systems and the platform would be developed by private actors while the standards and norms would be decided by the central administration: “interoperability standards by central administration authority. Platform (and other systems) developed by private companies (more efficient)” (Scholar). Similarly, other participants argued in favor of using the resources provided by the private sector. A collaboration with the BIG4 (private auditing services) was also suggested as a way to oversee the new structure: “I see a role for BIG4 to oversee such an organizational unit, e.g., by way of an externally invested internal audit function” (Private sector).

Third, a limited number of other respondents argued in favor of a new entity inspired by the SMALS model (not-for-profit government organization): “In my opinion, we need a central organization (like smals) that is independent of the various entities and free to make the most appropriate technological choices, but also free to review certain obsolete business processes” (Private sector).

A few participants also formulated some other recommendations, such as distinguishing the technical and governance aspects in this new entity: “It is necessary to distinguish the technical part (development of data services, data platform / meta data) from the governance part and coordination

of priorities" (Social security). Others mentioned that this new entity should act as a center of expertise that would assist other FPSs: "what is currently missing is a center of expertise to turn to, which can advise, monitor and assist in the development of projects..." (Justice). A somewhat decentralized approach was also proposed for the coordination, development, and monitoring of future digital projects in administrations: "Pure centralization will not work in practice, I think. Having an entity coordinating the common platform and creating a pool of specialists (business and IT working together) in each SPF could allow these exchanges of information both business and technical" (Finances).

The following figure presents a tag cloud that synthetizes the themes that were identified during the qualitative analysis of question 2.4.

Figure 12 - Tag cloud for question 2.4

3.3. SECTION 3 - LIMITING PUBLIC ACTORS' DEPENDANCE TOWARDS PRIVATE ACTORS

The third section of the Delphi survey aimed at bringing some possible answers to the issue of public actors' dependance towards private IT solution providers. Based on the results of the previous steps of the DIGI4FED research project, a series of possible solutions were presented to the participants. The first consists in promoting the internalization of digital skills through the development and technical management of a data exchange platform. The second solution consists in promoting the adoption of national or European solutions that meet strict data protection requirements. The following text box presents the short background piece that was presented to the survey participants:

> According to workshops and interviews, a central issue in the governance of the ecosystem of actors involved in the fight against fraud is **public actors' dependance towards private IT solution providers**. Public actors tend to lack the internal capabilities to develop their own systems and analysis tools. They rely on solutions provided by private actors and therefore have relatively little control over the development and use of these systems. This can cause issues with respect to the protection of personal data since private actors are likely to have access to this data (whose storage can also be problematic).
>
> The governance model could therefore ensure that public actors are strengthened by:
>
> - **Promoting the internalization of digital skills through the development and technical management of a data exchange platform**. One possibility could be to internalize technical skills by assigning a federal service (e.g., FPS BOSA or a new entity along the lines of Smals) with the task of developing and managing a common data exchange platform across administrations. This would strengthen internal skills while providing a solution that meets high standards in terms of transparency and data protection.
> - **Promoting the adoption of national or European solutions that meet strict data protection requirements**. Favoring data analysis or storage solutions developed by national (development of a Belgian cloud, for example) or European (AI4europe, ESSIF, EBSI, etc.) actors could help maintaining administrations' fraud-fighting capabilities while reducing their dependence on private solutions that are problematic in terms of personal data protection.

QUESTION 3.1

The first question of the third section of the survey is as follows: Which of the following statements best illustrates your view regarding the proposed solutions to limit the dependence of public actors towards private actors? Could you specify why? Possible answers are: They limit the dependence of public actors; They partially limit the dependence of public actors; They do not limit the dependence of public actors; There is no dependence of public actors; No opinion.

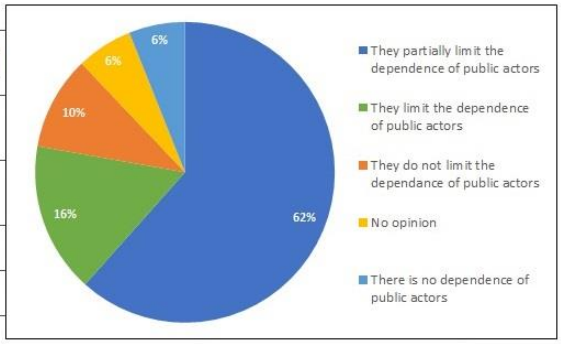
Short summary

A total of 31 participants answered this question. Overall, 16 % of participants agreed that the proposed solutions do limit the dependence of public actors. 61 % of participants considered that the proposed solutions only partially limit the dependence of public actors. 10 % considered that these solutions do not limit the dependence of public actors. 6 % of participants considered that there is no dependence of public actors and 6 % had no opinion. The following figure synthetizes participants' answers to question 3.1.

Figure 13 - Question 3.1 summary: do these solutions limit the dependence of public actors?

31 answers

e=They partially limit the dependence of public actors	19	61 %	
o=They limit the dependence of public actors	5	16 %	
n=They do not limit the dependence of public actors	3	10 %	
j=There is no dependence of public actors	2	6 %	
p=No opinion	2	6 %	



Qualitative analysis

In addition to these numbers, a thematic analysis of participants' supplementary answers allowed us to identify two main topics of discussion regarding the ability of the proposed solutions to limit the dependence of public actors towards private actors.

The first topic voiced by participants concerns the pivotal role and importance of private IT solutions providers in relation with the public sector. A significant number of participants stressed that the involvement of private actors remains and will remain inevitable for many reasons. Some participants mentioned the important financial resources at the disposal of some private actors. Such resources contrast with those of public actors who struggle to internalize competences and to maintain job attractiveness: "Internalization requires budget: it means attracting employees in competition with the private sector and is at odds with personnel savings in the government, which then has no choice but to work with external parties" (Federal Administration). Similarly, "in practice, it will still be necessary to rely on private providers of IT solutions because the government is not able to offer sufficiently attractive employment conditions to convince IT professionals to come and work for the government" (Regional administration). Other participants mentioned that, even if measures are taken in favour of the internalization of competences, a deep dependence to private technological solutions will remain: "First of all, technically, these programs are not created from new codes. These programs, whether they are created by the public or the private sector, are based on the foundations of the big machines of GAFAM" (Union). Similarly, "for certain niche solutions a dependence on private actors will remain" (Social security) and "Private IT solution providers will always be present in the learning phase of their tool" (Finance). More generally speaking, many participants consider that some private IT solution providers have gained such a technological edge that it would be difficult for national or European players to compete with them: "Some solutions proposed by foreign players are difficult to compete with. They do not always have a national or European equivalent" (Not-for-profit organization).

Several participants also affirmed that they tend to consider private IT solution providers as generally more competent and reliable than public actors, including on the topics of data security and personal data protection: "Private actors are often much more concerned about respecting the private data of their clients, and in this case the citizens, than the public actors themselves. For me, the debate is

about the competence of the different actors and especially about the respect by the profession of the data security constraints" (Private sector). Similarly, "Inspectorates have a big dilemma if they work with digital personal data: on the one hand, existing digital applications that are often very useful may not be used because the data is stored outside the EU (GDPR). On the other hand, the security offered by an in-house application can never compete with the security offered by those big software vendors. Acting legally correct (GDPR) actually offers the least guarantee of safe handling of personal data" (Social security).

Given these elements, several participants argued in favour of a collaboration between private and public actors: "I think it should always be a collaboration between government and private actors, collaboration is going to give the most results" (Private sector). Similarly, "Digital expertise is scarce in the marketplace, so partnering with the private sector is evident. Resources must be obtained where they are available" (Private sector). For some, a concern was that an independent public sector might jeopardize the collaboration with the private sector. Bolstering in house projects and the internalization of expertise would result in a form of self-centredness of the public sector and an increased dependence on a limited number of internal bodies: "Internalising technical competences by entrusting a federal service with the task of developing and managing a data exchange platform common to the administrations can only lock in the organisation, increase dependence on a small number of bodies and reduce the possibility of collaboration with private actors" (Private sector). The adoption of open standards and technologies was seen as a way to reduce dependence while maintaining a form of collaboration with private actors: "The use of open standards, open technologies, and internal developments, allow the government to engage private partners, but not become dependent on one or the other" (Finances).

The second main topic voiced by participants concerns the obstacles that are faced by the public sector in achieving a reduction of its dependence towards private actors. According to participants, the most important obstacle faced by public authorities is the lack of internal skills and expertise: "If there is not enough in-house expertise (and time) available to "challenge" them, the impact is more limited in practice" (Federal administration). "It will be a challenge in any case to roll out, for example, data storage in one's own cloud management" (Private sector). Respondents often mentioned the need for a greater internalization of expertise in order to reduce dependence: "More in-house sourcing of technical knowledge and more sovereignty over in-house technological solutions reduces the dependence of the government on private players" (Federal administration); "Developing certain digital skills internally will benefit independence" (Social security). This expertise issue is closely linked with the lack of resources within the public sector: "too little public investment in R&D" (Finances). According to participants, this lack of resources also affects administrations' ability to maintain job attractiveness and internalize IT expertise: "It will not be possible to internalize this at FPS BOSA either, unless there are more flexible working conditions there (higher pay, flexible hours, fringe benefits, etc.)" (Finances); "Internalization requires budget: it means attracting employees in competition with the private sector and is at odds with personnel savings in the government" (Federal administration).

Along with a greater internalization of IT skills, some participants suggested to resort to alternate IT solutions to limit the dependance towards private actors. Some argued in favor of solutions developed by European actors: "The internalisation of digital skills within the government and the use of national or European government-provided and developed solutions (such as PEPPOL) are indeed ways of

reducing dependence on private providers of IT solutions" (Regional administration). Other participants advocated for open-source solutions to limit public actors' dependence: "More sovereignty can be achieved here by choosing open source (linux, android, open office applications) and not closed source as is still too often done" (Federal administration).

The following figure presents a tag cloud that synthetizes the themes that were identified during the qualitative analysis of question 3.1.

Figure 14 - Tag cloud for question 3.1

QUESTION 3.2

The second question of the third section of the survey is as follows: Should the solutions proposed by national or European actors be preferred? Why or why not?

Qualitative analysis

A thematic analysis allowed to identify three main categories of answers to this question. First, a considerable number of participants voiced their preference in favour of both national and European IT solutions: "It is better to reuse something that already exists at a national/European level than to reinvent it" (Federal Administration). "Solutions by national and European players are advisable" (Social security). Participants often argued that, ideally, both European and national IT solutions should be compliant with GDPR regulations. This means that both options are deemed adequate regarding the issue personal data protection: "Yes, in order to promote the respect of privacy rules. US and Chinese companies are subject to national rules contrary to the GDPR and this even if they are established on EU territory. Favouring national and/or EU actors makes it easier to ensure compliance with the GDPR" (Justice). These European and national solutions "will be able to better integrate national and European standards 'by design'" (Not-for-profit organization). Other participants argued that privileging both solutions should allow to participate to a common (European) strategy while keeping an equilibrium between standardization and the respect of local specificities: "in the context

of the "open strategic autonomy" that is now a new priority of the European Union, recourse should preferably be had to national or European private providers of IT solutions (e.g. GAIA-X), rather than to U.S. private providers (e.g. AWS or Azure) as is still the case today" (Regional administration). Similarly, "In terms of posting (European directive), each country develops different tools to promote the proper application of the directive and ensure compliance with the regulations. Of course, the social specificities of each state must be taken into account, but there is also a competition to develop the best tool that could be applied to the whole EU" (Social security).

Second, some participants argued in favour of European solutions. These respondents mentioned that the GDPR legislation is an adequate groundwork on which to build new IT solutions for public services. They also stressed that the EU has sufficient resources for the development of such tools: "It seems to me that it would be beneficial to integrate this at a European level. The GDPR legislation is a European matter which ensures that there is a lot of knowledge available at the European level. Partly because the GDPR was introduced at a European level, the regulations are the same at a national level. By introducing this at the European level a level playing field is created and strong efficiency gains are achieved. In addition, I should point out that European policy has made a strong choice to invest in digital innovations. So, these policies are very much in line with each other" (Social security). "Indeed, best on a European level: own GDPR legislation and large enough to develop good applications" (Social security). Other participants mentioned the existence of several promising European projects that should play an important role in achieving IT sovereignty in the EU: "It is a question of European sovereignty, which is dealt with at this level (among others via projects such as GAIA-X, AI, etc...)" (Regional administration); "We should preferably rely on national or European private IT solution providers (e.g., GAIA-X)" (Regional administration); "In my opinion, European decentralized solutions can certainly contribute" (Private sector).

Third, some other participants voiced their preference for national IT solutions. In their opinion, opting for European solutions appears too complex and far-fetched. National IT solutions seem the most realistic to these participants: "Rather national players, it's complicated enough as it is. European players seem to me to be completely utopian and very, very long term" (Mutuality); "The national level would already be a big step forward before thinking about European players" (Social security). Others voiced their preference for national solutions, but with the possibility of finding other solutions elsewhere if they are more cost-effective: "preference to national actors but it is not mandatory, with encryption we can also go outside Europe if more effective / efficient ... cheaper" (Regional administration).

Although most participants answered in favour of one of the options mentioned above, some declared being open to all options as long as citizens' interests are respected: "Whatever the system, each individual must have control over his or her data" (Union). Other participants also formulated some caveats and precautions when opting for a European or a national IT solution. According to them, it is first important to make sure that the solution is adapted to the challenge at hand and to the needs and skills of the end users: "If these are available, sufficiently mature and equally user-friendly then this is certainly where the preference may lie. Currently, this is still often not the case" (Federal administration). Another precaution would be to make sure that public authorities keep an eye in the development of new IT solutions and ensure their compliance with standards: "Either way, as long as the government watches over compliance with the predefined standards and maintains control over

developments. It is up to the government to determine this, not the other way around (because then they might sell all kinds of things that the government does not need)" (Finances). Finally, some participants warned against the risk of creating a form of dependence towards national or European actors: "you shift the dependence from, say, Smals to dependence on national or European players. The problem is that the task of the 'external consultant' is never completed, because they are also used for maintenance of their solutions" (Finances).

The following figure presents a tag cloud that synthetizes the themes that were identified during the qualitative analysis of question 3.2.

Figure 15 - Tag cloud for question 3.2

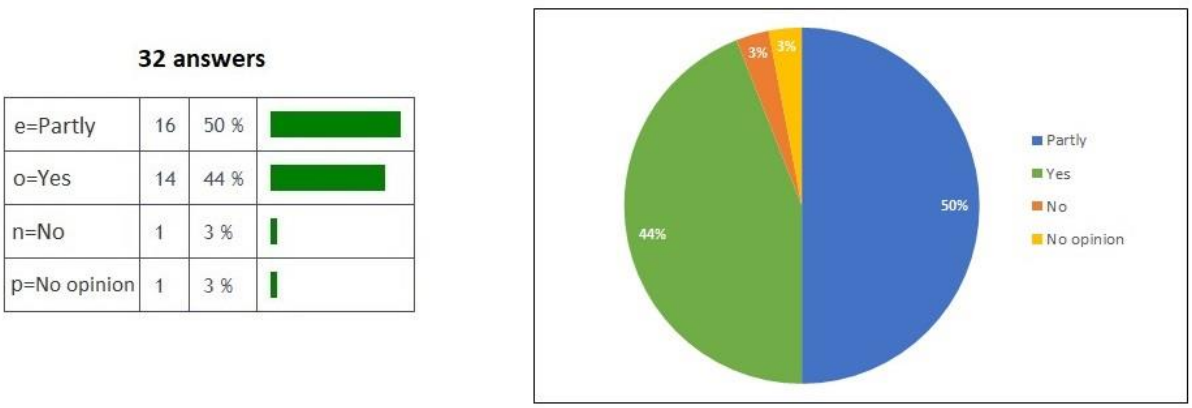
QUESTION 3.3

The third question of the third section of the survey is as follows: Do you think that a federal service would be able to assume the development and the technical management of a new data exchange platform? Could you specify why? Possible answers are: Yes; Partly; No; No opinion.

Short summary

A total of 32 participants answered this question. Overall, 44 % of participants agreed that a federal service would be able to assume the development and the technical management of a new data exchange platform. 50 % of participants only partially agreed that a federal service would be able to assume this task and 3 % did not agree with this idea. 3 % had no opinion. The following figure synthetizes participants' answers to question 3.3.

Figure 16 - Question 3.3 summary: can a federal service assume the development and management of a new data exchange platform?



Qualitative analysis

In addition to these numbers, a thematic analysis of participants' supplementary answers allowed us to identify four main topics of discussion regarding federal services' ability to assume the development and the technical management of a new data exchange platform. First, several respondents argued that the development and the technical management of a new data exchange platform should be entrusted either fully, or in part, to public authorities. To that regard, most agree that federal services should work in collaboration with the private sector which can provide much-needed expertise and resources: "No doubt external consultants will have to be hired to help set up such a platform, but the maintenance could be done entirely by the federal service, when it is not buying a product from the consultants, but knowledge. With knowledge, you can do what the consultants do" (Finances). In other words, these respondents suggest that federal services should be "joining forces with a private partner where there is a lack of expertise" (Not-for-profit organization). However, some do mistrust private actors and argue in favour of a fully autonomous development of the platform: "No private institution aims to make the government function better. So, there is no alternative but to take matters into our own hands as a government" (Social security).

Second, a significant number of participants mentioned the constraints that could negatively affect the development and subsequent management of such a platform by federal services. Among these constraints are the limited resources of the public sector: “It will take time and money, but it is a project that will make life easier for all actors. Politicians must want it and give real means to such a long-term project” (Social security); “It is necessary to see the means at disposal to guarantee this safely” (Private sector). Another commonly evoked constraint is the lack of internal expertise: “the public service must have the data skills to manage and develop the necessary services” (Social security). Participants argue that federal services should be able to take care of this task provided that they can rely on a “service with the necessary knowledge and up-to-date technical baggage” (Finances). Some participants also mentioned the lack of political will as a possible detrimental factor: “Politicians must want it and give real means to such a long-term project” (Social security). In other words, “everything depends on the priority of the implementation of this platform” (Finances).

The third topic voiced by respondents is the existence, within administrations, of systems that they consider close, or similar, to the proposed data exchange platform. As for the questions 2.2 and 2.3, some participants argued that such a data exchange platform system already exists (at least partially) at the federal level: “The FPS BOSA DG DT already offers such a platform for data exchange with the federal service bus (FSB), so it seems logical to us to build on this to build a more comprehensive platform for data exchange” (Regional administration). These respondents also mention the existing service integrator which already serves the purpose of facilitating the sharing of data between administrations at the federal level: “There is already a service integrator. The expectations should be specified and the BOSA service integrator should be used for example” (Federal administration). A suggestion is thus the development of public *data lake* rather than a shared data exchange platform: ‘It is necessary to create a public 'data lake'“ (Federal administration).

Finally, a few participants provided some advice regarding the development and management of the proposed platform. For instance, it was mentioned not to underestimate the costs and challenges associated with keeping the platform up-to date from a technical standpoint: “the problem of being able to stay up to date concerning technical evolutions is difficult to overcome in the administration (expenses and costs in training hours + daily work makes it quickly impossible to follow the evolutions)” (Justice). Other participants argued that the federal development of the platform should be made in collaboration with other levels of government: “In connection with federated entities including DNA. Example, ODWB.” (Private sector).

The following figure presents a tag cloud that synthetizes the themes that were identified during the qualitative analysis of question 3.3.

Figure 17- Tag cloud for question 3.3

3.4. SECTION 4 - VALUES AND DATA GOVERNANCE

The fourth section of the Delphi survey aimed at bringing some possible answers to the limited acceptability of new fraud fighting tools among companies and citizens and to the difficulties in organizing the digital governance in a context where financial resources are lacking. Based on the results of the previous steps of the DIGI4FED research project, a series of possible solutions were presented to the participants. The first solution consists in improving the communication about how the system works. The second solution consists in allowing public authorities to take on the role of key regulators in data governance. The third solution consists in stimulating private actors to provide administrations with efficient tools without creating additional financial constraints. The following text box presents the short background piece that was presented to the survey participants:

Several issues pertaining to the expectations of administrations and end users have been identified. The workshops and interviews have underlined **the limited acceptability of new fraud fighting tools among companies and citizens**. These new tools (AI in particular) tend to be negatively perceived, and their acceptance is difficult as long as their added value is not directly perceived. On their part, public actors are experiencing **difficulties in organizing the digital governance in a context where financial resources are lacking**. Due to budgetary constraints, administrations tend to choose private IT solutions, which are less costly but sometimes problematic in terms of confidentiality (Google Analytics until recently, for example).

The governance model could therefore ensure that these expectations are met by:

- **Improving the communication about how the system works**. To improve the acceptability of the new tools, one solution could be to deploy more communication and pedagogical efforts in the justification of the choices that govern the large-scale use of personal data in the fight against fraud.
- **Allowing public authorities to take on the role of key regulators in data governance**. Public managers could be granted the ability to control the access to personal data stored on the common data exchange platform mentioned earlier. They could then establish specific rules for actors who wish to access the data for commercial or public purposes. They could also choose to share some specific data with European counterparts to strengthen transnational anti-fraud capabilities for example.
- **Stimulating private actors to provide administrations with efficient tools without creating additional financial constraints**. The public managers of the data exchange platform could decide to authorize the use of some carefully anonymized personal data to private actors who wish to develop new predictive tools using this data as training data. The newly developed tools could then be integrated by administrations, thus reinforcing their fraud detection capabilities without requiring additional resources the immediate future.

QUESTION 4.1

The first question of the fourth section of the survey is as follows: Do you think it is relevant that the public managers should endorse the role of key regulators in data governance? Could you specify why? Possible answers are: Yes; Partly; No; No opinion.

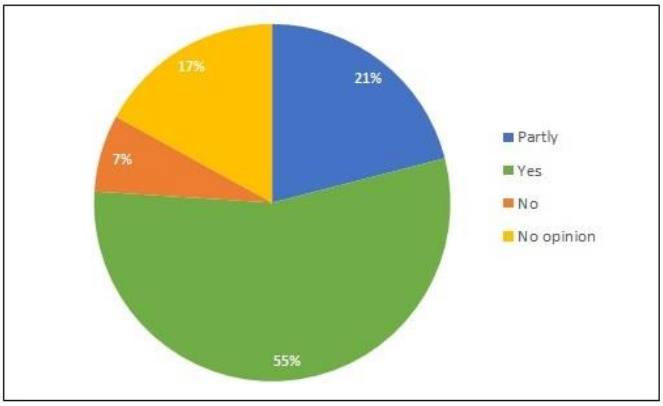
Short summary

A total of 29 participants answered this question. Overall, 55 % of participants agreed that it is relevant that the public managers should endorse the role of key regulators in data governance. 21 % of participants only partially agreed with this idea while 7 % did not agree. 17 % had no opinion. The following figure synthetizes participants' answers to question 4.1.

Figure 18 - Question 4.1 summary: is it relevant for public managers to endorse the role of key regulators in data governance?

29 answers

o=Yes	16	55 %	
e=Partly	6	21 %	
p=No opinion	5	17 %	
n=No	2	7 %	



Qualitative analysis

In addition to these numbers, a thematic analysis of participants' supplementary answers allowed us to identify three main topics of discussion. Many respondents were concerned with the nature of public sector's role in data governance. First, a considerable number of participants voiced that it is indeed the role of public actors to be in charge of the regulation of data governance: "It is the role of the public sector to assume this regulatory role" (Social security). Similarly, "someone has to manage the data. It is better for the citizen that a civil servant does this than a private company" (Finances). Other stressed that EU member governments are already expected to assume this role: "With the Data Governance Act and Data Act proposed by the European Commission, an important part of the responsibility for setting up the appropriate data governance rules is placed on the government. The government does indeed have an important role to play here, as a provider of a lot of open data and as an institution that should set a good example in the appropriate use of (personal) data" (Regional administration).

Second, some of participants did formulate some misgivings regarding the central role of the public managers in regulating data governance. Indeed, some argued that public authorities should not bear these responsibilities alone and that the private sector and/or citizens should be associated to the data regulation process: "the private sector cannot be the regulator but there must be collegiality and representativeness of user entities in the regulation (not a single manager)" (Justice). Similarly, many argued that citizens should be associated to the process: "the citizen/company must have a say in what is done with their data - the end cannot justify the means" (Private sector). In other words, this "must be a shared responsibility between government and data subjects" (Federal administration). Additionally, leaving the citizens out of the process would have a negative impact on trust: "It is not certain that the citizen's trust will be strengthened if the possibility is left solely to public managers to determine the rules of data exchange" (Not-for-profit organization).

Another opinion was that the regulative task should not be entrusted to public authorities altogether: "this role should be fulfilled by a control body that is totally independent of the public services and political power. In the same principle of the separation of powers at state level. Otherwise, we are

confronted with actors who are judge and jury and this does not give confidence and does not guarantee independence and security" (Private sector).

Finally, the last topic concerns some other observations made by participants. One of such observations was that the notion of managers / regulators of governance is sometimes unclear: "It depends on what is meant here by 'government managers'. I assume that it does not refer to individuals, but to (collaborating) managers. The government as a whole should of course be the regulator" (Social security). Other participants were unsure about the scope of the discussion about data governance: "The scope of this discussion needs to be better described. The method and institutional approach will be derived from this scope" (Federal administration). Another observation was that, if public managers are to endorse the role of main regulators in data governance, there is a need for a strong legal framework to avoid possible pitfalls: "It all depends on how this is implemented. What is the legal framework in which they operate, who defines it,... It is not certain that the confidence of the citizen will be strengthened if the possibility is left solely to public managers to determine the rules of data exchange" (Not-for-profit organization).

The following figure presents a tag cloud that synthetizes the themes that were identified during the qualitative analysis of question 4.1.

Figure 19- Tag cloud for question 4.1

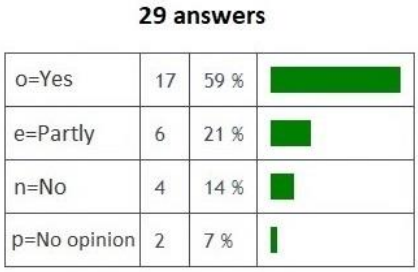
QUESTION 4.2

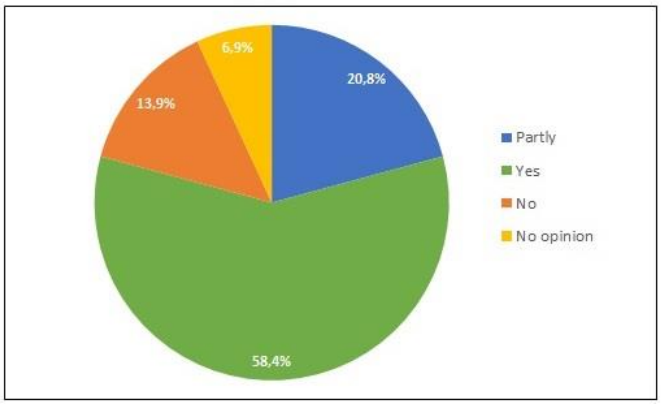
The first question of the fourth section of the survey is as follows: Do you think that a (supervised) contribution from private actors could help administrations to adapt and maintain their fraud detection capacities? Could you specify why? Possible answers are: Yes; Partly; No; No opinion.

Short summary

A total of 29 participants answered this question. Overall, 59 % of participants agreed that a supervised contribution from private actors could help administrations. 21 % of participants only partially agreed with that idea while 14 % did not agree. 7 % had no opinion. The following figure synthetizes participants' answers to question 4.2.

Figure 20 – Question 4.2 summary: can private actors help adapt and maintain the fraud detection capacities of administrations?





Qualitative analysis

In addition to these numbers, a thematic analysis of participants' supplementary answers allowed us to identify two main topics of discussion. The first aspect brought by respondents was the pivotal role of the private sector. A significant number of participants stressed the necessity of a cooperation between the actors of the public sector and the private sector. This position was put forward for several reasons. Some participants mentioned the superior technical expertise of private actors: "From an operational point of view, the contribution of the private sector's expertise can only be positive in the objective of developing tools to fight fraud" (Social security). Similarly, "Fraud detection seems to me to be a public task par excellence. Private actors can support it (making technology available that is used by public services)" (Finances). Participants also mentioned the important resources of private actors. Others stressed that administrations could largely benefit from the talent and innovations brought by the public sector: "For various reasons, the talent is in the private sector. If it were possible to find a model in which this talent could be used in a controlled way to combat fraud, that would be a great gain" (Finances). Similarly, "collaboration with private actors can only be beneficial for the development of 'innovative' solutions" (Private sector). If set up properly, these participants also considered the use of carefully anonymized personal data as training data for private actors as a promising prospect: "If set up properly and taking into account absolute data anonymization" (Federal administration). Similarly, this data "can be used as a 'test environment'; be careful with the encryption of anonymous data." (Social security).

The second main topic voiced by participants was the need for caution when collaborating with the private sector. Stakeholders stressed that prudence is required when dealing with private actors. Precautions, such as the strict anonymisation of personal data, are needed. In other words, it is important that the "contribution of private actors is always controlled and takes place in a strict legal-

technical framework" (Federal administration). Similarly, "It is important, however, that this is done in a controlled way and that private parties do not have access to non-anonymised personal data under any circumstances" (Social security). Some participants also expressed their clear distrust at private actors and considered their involvement in new fraud-fighting tools development as unwanted: "outsourcing parts seems to me to go too far. The problem is that private actors serve different (own) interests than the public ones" (Finances). Similarly, "people are people and individual interests will always, at some point, take precedence over the collective interest. This exists in the public sector, but it can be controlled. It is more difficult in the private sector, where profit is an end in itself" (Union).

The following figure presents a tag cloud that synthetizes the themes that were identified during the qualitative analysis of question 4.2.

Figure 21- Tag cloud for question 4.2

QUESTION 4.3

The first question of the fourth section of the survey is as follows: Do you think that the proposed solutions allow for a governance of data that can be understood by all actors concerned by the protection of personal data? Could you specify why? Possible answers are: Yes; Partly; No; No opinion.

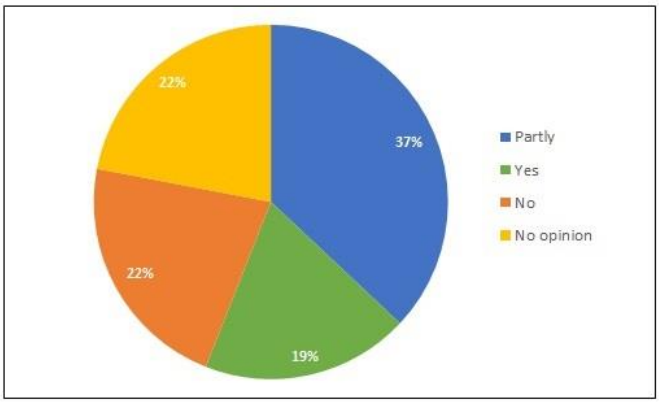
Short summary

A total of 27 participants answered this question. Overall, 19 % of participants agreed that the proposed solutions allow for a governance of data that can be understood by all actors. 37 % of participants only partially agreed with that idea while 22 % did not agree with this idea. 22 % had no opinion. The following figure synthetizes participants' answers to question 4.3.

Figure 22 - Question 4.3 summary: do these solutions allow for an understandable data governance for all data protection actors?

27 answers

e=Partly	10	37 %	
p=No opinion	6	22 %	
n=No	6	22 %	
o=Yes	5	19 %	



Qualitative analysis

In addition to these numbers, a thematic analysis of participants' supplementary answers allowed us to identify three main topics of discussion. The first aspect brought by respondents was the importance of transparency and communication with citizens. A number of participants argued that, in order to achieve a clear and understandable data-governance, a better communication would be needed to explain to citizens how their data is handled by public authorities and for what purposes: "this is not enough in my opinion. Trust in public services is very low among citizens, so they will not trust a few officials to handle their data properly without explanation" (Finances). Similarly, "improving communication on data use is a way to give citizens and businesses more confidence in how their (personal) data are used (for fraud prevention)" (Regional administration). In general, for those participants "it would seem that an additional communication effort is needed" (Federal administration). To that end, participants also stressed the need for transparent communication. Citizens should be clearly and precisely informed on who uses their data, how, and with what purposes: "The simplest way would be to say / there are servers on which your data is stored; unless you have a warrant from a judge, that place is, like your home, inviolable. To move that data from one place to another, beyond a procedure covered by a judge, permission is needed. You are the owner of this data, so it is accessible to you at all times. This service and this protection are provided by the FPS ... and the legislation on the protection of privacy of ... That's much clearer, don't you think?" (Union).

The second topic voiced by participants was the need for a clear legal framework and procedures to allow for an understandable data governance: "this must be analysed in depth and a whole series of guarantees, safeguards, procedures, etc. must be provided for" (Justice). Similarly, there is a need to "create the right laws and regulations that can adequately frame B2B, B2G and G2B data sharing" (Regional administration).

The last topic concerns some other observations made by participants. Such an observation was that citizens and businesses should also be actively associated to the construction of the governance model: "The first actors concerned by the protection of personal data are the citizens/businesses. They must have an active role in defining a governance model" (Not-for-profit organization). Another observation was the need for simplicity of the model. Complex solutions are often less accepted than simple ones: "Facebook has been offering fine-grained data control for years. Few people use it. If it works without effort, even if it is disadvantageous, people will still choose the easy solution" (Private

sector). Some participants also mentioned the need for the appropriate knowledge and expertise among some actors: communicating on data governance "requires a high degree of technical knowledge among some actors" (Federal administration).

The following figure presents a tag cloud that synthetizes the themes that were identified during the qualitative analysis of question 4.3.

Figure 23 - Tag cloud for question 4.3

QUESTION 4.4

The first question of the fourth section of the survey is as follows: Do you think that better communication about the use of new technologies in the fight against fraud could lead to a better understanding and acceptance of these tools by citizens and companies? Could you specify why? Possible answers are: Yes; Partly; No; No opinion.

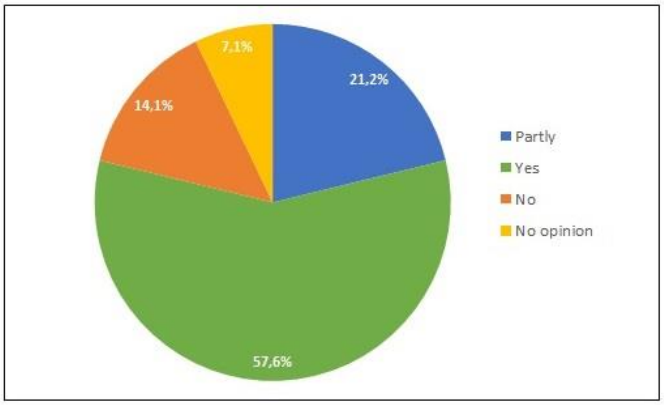
Short summary

A total of 28 participants answered this question. Overall, 57 % of participants agreed that a better communication about the use of new technologies in the fight against fraud could lead to a better understanding and acceptance of these tools by citizens and companies. 21 % of participants only partially agreed with that idea while 14 % did not agree. 7 % had no opinion. The following figure synthetizes participants' answers to question 4.4.

Figure 24 – Question 4.4 summary: would better communication about new technologies lead to a better understanding and acceptance?

28 answers

o=Yes	16	57 %	
e=Partly	6	21 %	
n=No	4	14 %	
p=No opinion	2	7 %	



Qualitative analysis

In addition to these numbers, a thematic analysis of participants' supplementary answers allowed us to identify three main topics of discussion. The first aspect brought by respondents was the importance of a clear and transparent communication with citizens and businesses. Many participants stressed that a clear communication would probably contribute to a better understanding and support among citizens and businesses: "better communication has only advantages. It will therefore certainly lead to a better understanding and more support among private actors" (Social security). Similarly, "if (when deploying the latest technology) the message is that the government is doing 'everything it can' to combat fraud, the public will accept this better than not deploying new technology at all and saying: 'we'll make do with what we have'" (Social security). In other words, "better communication about the use of new technologies to combat fraud can help citizens and businesses better understand the purpose of these technologies and exactly what data are used to combat fraud" (Regional administration). This would in turn contribute to a greater endorsement of these technologies. Some participants also argued that good communication should be characterized by transparency. Such transparency would then contribute to trust and acceptance among citizens: "Transparency creates trust, understanding and acceptance" (Private sector); "Transparency is essential in creating trust among citizens" (Federal administration). Transparency was also considered beneficial for fraud-fighting purposes: "All inspectorates know that transparency can prevent a lot of fraud" (Social security).

The second main topic voiced by participants concerned the limits and weaknesses of communication. Indeed, some respondents argued that communication with citizens and businesses would have a limited impact if the added-value and benefits of new fraud fighting tools are not put forward: "too much emphasis is placed on negative aspects (combating fraud), reinforcing the perception of a controlling government, instead of focusing on positive consequences for citizens (better assistance to individual needs)" (Federal administration). Similarly, "In addition to understanding the models and the operations carried out, the citizen must above all have the means to understand what the added value of these tools is for him. All too often, the added value seems to be indirect for them" (Social security). Another aspect brought by some respondents was that a better communication would not necessarily contribute to a better comprehension among citizens: "I don't think that communication

will lead to a better understanding" (Finances). Some other participants also mentioned the defiance and preconceived ideas regarding public authorities. Such mistrust might impede proper communication on new fraud fighting tools: "the image is tenacious, and the citizen always finds that one goes more into his pocket than where the fortune is... more communication can also have an opposite effect for some (and induce more mistrust because they would have the impression that one does much more to control them)" (Justice). Similarly, "it is not necessarily the new technologies used that are frightening but the use that the public service can make of them that is worrying for the citizen" (Private sector). It was also noted that communication might only be a part of the solution. For instance, giving to citizens and businesses the choice of participating or not could help in fostering acceptance: "Communication can contribute to this. However, it is the choice/freedom that should be given to the citizen/business that will allow acceptance. Imposed solutions are rarely welcomed and respected" (Private sector).

Finally, the last topic concerns some other observations made by participants. One of such observations was that priority should not go to the development of new tools and a better communication. Instead, priority should be given to allocate sufficient resources to the services involved in the fight against fraud so that they can do their job properly: "we must put the means where they belong in the fight against fraud (especially tax fraud) and not believe that technology is the solution to everything" (Union). Another observation was that decentralized approaches to data management tend to be safer than centralized ones and that this should be communicated to citizens: "any computer system is by definition susceptible to hacking and therefore the more centralized the data, the more dangerous it is for the citizen. Risk that the data is stolen or also in some cases destroyed" (Private sector).

The following figure presents a tag cloud that synthetizes the themes that were identified during the qualitative analysis of question 3.4.

Figure 25 - Tag cloud for question 4.4

3.5. SECTION 5 - IMPROVING THE EXPLAINABILITY OF THE ANALYSIS PROCESS

The sixth section of the Delphi survey aimed at bringing some possible answers to the difficulties in ensuring the explicability of decisions based on predictive algorithms. Based on the results of the previous steps of the DIGI4FED research project, a series of possible solutions were presented to the participants. The first solution consists in promoting the adoption of new predictive tools that allow for a better traceability of analyses. The second solution consists in improving the reliability of these new tools by conducting pilot experiments in a secure environment. The following text box presents the short background piece that was presented to the survey participants:

> The workshops and interviews suggest that the **difficulty to ensure the explicability of decisions based on predictive algorithms** is a central issue presiding over the technological choices for data analysis in the fight against fraud. AI solutions can be effective when used in the fight against fraud. However, they can also result in blackboxes by increasing the opacity of the data analysis processes. As a result, the explanation of fraud related decisions to citizens and companies can be undermined.
>
> The governance model could therefore ensure to improve the explicability of analysis processes by:
>
> - **Promoting the adoption of new predictive tools that allow for a better traceability of analyses**. It would be possible to develop and adopt explainable AI (XAI) solutions which allow to explain the relative weight of certain data in the results obtained by the analysis. In the same way, some progresses are being made in the decoding of blackbox algorithms, thus indicating that it would be possible to improve the explicability of decisions resulting from such algorithms.
> - **Improving the reliability of these new tools by conducting pilot experiments in a secure environment**. Such experiments could be conducted using anonymized training data provided by the public managers of the data exchange platform. Conducted on a large scale, such an approach could significantly enhance the reliability and technological maturity of the proposed solutions. These experiments could also be integrated into public procurement processes to test new solutions before they are introduced in administrations. However, the development and adoption of such tools should be consistent with the principle of proportionality defended by the GDPR and should minimize the risks of socio-economic inequalities reproduction.

QUESTION 5.1

The first question of the fifth section of the survey is as follows: Do you think that the proposed solutions can improve the explainability of decisions based on AI? Could you specify why? Possible answers are: Yes; Partly; No; No opinion.

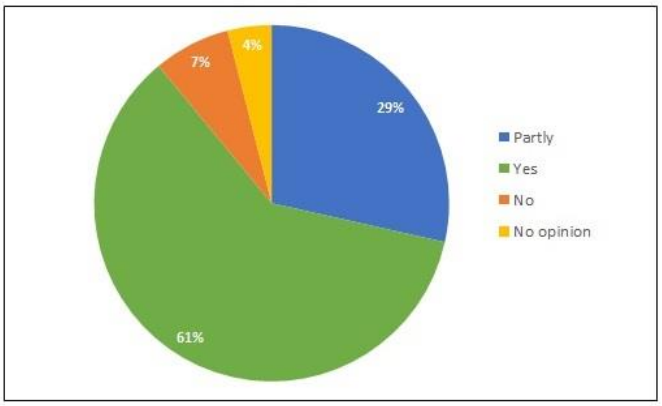
Short summary

A total of 28 participants answered this question. Overall, 61 % of participants agreed that the proposed solutions can improve the explainability of decisions based on AI. 29 % of participants only partially agreed that they can improve explanability and 7 % did not agree with this idea. 4 % had no opinion. The following figure synthetizes participants' answers to question 5.1.

Figure 26 - Question 5.1 summary: can the proposed solutions improve the explainability of AI based decisions?

28 answers

o=Yes	17	61 %	
e=Partly	8	29 %	
n=No	2	7 %	
p=No opinion	1	4 %	



Qualitative analysis

In addition to these numbers, a thematic analysis of participants' supplementary answers allowed us to identify five main topics of discussion. The first aspect discussed by respondents was the effect of these new AI solutions on explainability of fraud related decisions. On that regard, a significant number of participants agreed that the proposed solutions would likely help in improving explainability: "XAI (explainable AI) is in any case a step in the right direction in the selection of potentially fraud-sensitive observations" (Social security). Similarly, XAI "helps to understand how AI arrives at the given result, so that the ethics of the algorithm can also be checked" (Finances).

Second, some participants stressed the difficulties and constraints associated with an improved explainability of fraud decisions. Some participants warned that new explainable fraud detection techniques could trigger a process of adaptation among fraudsters: "Updating all investigation methods could open the door to new frauds or ways to circumvent the rules" (federal administrations). Another observation was that an improved explainability of algorithms and fraud-related decisions does not necessarily mean that such explanations are understandable: "Being able to explain complex AI algorithms is one thing but making them understandable while taking into account an analysis of all the possible adverse effects, for example, is a challenge that has no simple solution" (Federal administration). Finally, it was also mentioned that such an improved explainability is not necessarily needed. In this view, the results are more important than the process leading to the decision: "However, in my view it is not always necessary to be able to explain why a model makes a certain choice. In that case, I think it should be sufficient to look at the results of the model" (Finances).

Third, participants discussed the technical validity of the proposed solutions. Some respondents were concerned regarding the technical maturity of XAI solutions and in vitro experiments, arguing that their validity was still to be established: "they are both still the subject of active academic research, so it is not yet clear whether these two approaches will be enough" (Regional administration). More specifically on XAI: "It remains to be seen in practice, as on the technical level AI has made relatively little progress in recent years. It is above all the computing capacity and the mass of available data that have evolved, but the problems inherent in the use of AI (machine learning in particular) have not changed for 30 years. We must remain attentive to these new technologies, which are not yet fully mature" (Social security).

Fourth, participants debated over the skills and expertise needed to deploy these solutions. Although some considered that these solutions are within the reach of public authorities, other participants were concerned by the complexity of the proposed solutions: “The proposed solution seems very complex and is something for a scientific environment” (Social security). An argument was also that the expertise needed to understand these tools is lacking in both the administrations and the population: “but I fear that no 10% of the population will ever grasp this analysis (XAI) ...” (Social security).

Finally, the last topic concerns some other observations made by participants. Among those observations was the necessity to keep humans actively involved in the monitoring and follow-up of fraud detection processes that rely on AI: “it is very important to keep 'human' control after an AI analysis, etc. The important thing is to be able to use the power of AI, datamining, etc. while being able to explain explicitly to the agent what the analysis is based on (business criteria, etc.). And on the basis of these elements and a verification of one or other element, the agent will make a decision on what to do with the selected cases” (Finances). For that purpose, it is also important to rely on a sound legal framework: “It should be noted, however, that all of this must be legally verified. Fraud is still a fact that an observation does not adhere to the predefined rules. Fraud, therefore, is a fact that is controlled according to a specific context and its rules (a black and white story)” (Social security).

The following figure presents a tag cloud that synthetizes the themes that were identified during the qualitative analysis of question 5.1.

Figure 27 - Tag cloud for question 5.1

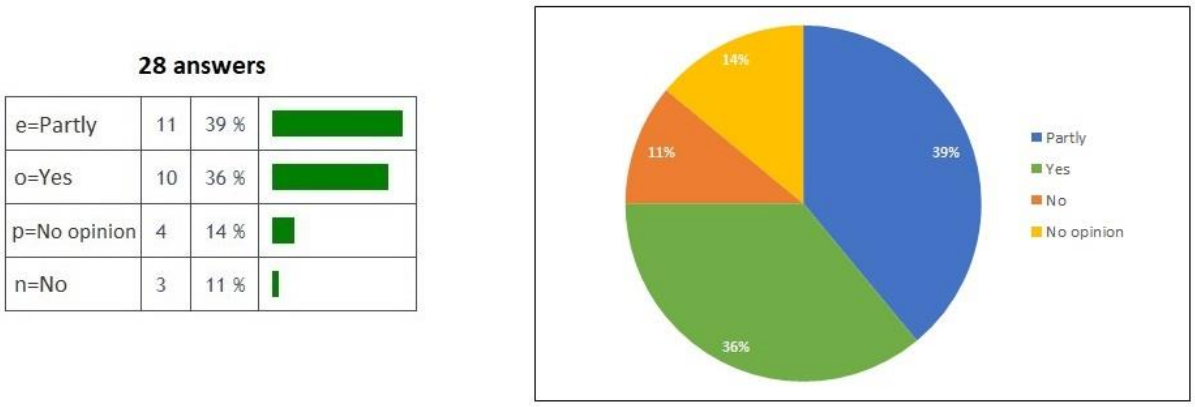
QUESTION 5.2

The second question of the fifth section of the survey is as follows: Do you think that the development and implementation of these new, explainable, tools is within the reach of the different actors involved? Could you specify why? Possible answers are: Yes; Partly; No; No opinion.

Short summary

A total of 28 participants answered this question. Overall, 36 % of participants agreed that development and implementation of these new, explainable, tools is within the reach of the different actors involved. 39 % of participants only partially agreed that this is within the reach of those actors and 11 % did not agree with this idea. 14 % had no opinion. The following figure synthetizes participants' answers to question 5.2.

Figure 28 – Question 5.2 summary: is the development and implementation of explainable tools is within the reach of the different actors?



Qualitative analysis

In addition to these numbers, a thematic analysis of participants' supplementary answers allowed us to identify three main topics of discussion. The first aspect voiced by respondents was the degree of expertise of the involved actors in view of achieving feasibility. Some argued that developing and implementing these new tools should be within the reach of the involved actors provided that they have sufficient skills and expertise. As such, "a period of adaptation and learning" (Federal administration) would inevitably be needed for the services who would adopt these new tools.

However, although creating these tools should be theoretically possible, finding the adequate expertise and skills in the population remains a difficult task according to some participants: "Yes, a lot is possible. However, this field is still in its infancy and there is a great shortage of specialized professionals. There is a strong focus on this within the educational system and the labor market. Unfortunately, no adequate solutions are visible in the medium term" (Social security). This issue is even more pronounced in the public sector, which is not ready for such tools according to a few other participants: "Something complex is difficult to explain. Something explainable is not too complex. For now, government is not ready for complex models" (Finances). Some others simply deemed this approach "too complex" (Social security) for it to be viable.

The second main topic of discussion concerned the technical validity of such a proposition. Some participants questioned the maturity of XAI, arguing that the validity of such systems was not yet demonstrated, let alone for such a use case: “It has yet to be demonstrated by academic research that for certain types of AI (e.g., deep learning) it is indeed possible to design and build better traceability of their operation and their results. If this is indeed possible, the developers of such AI solutions must be able to build this into their solutions, and the principals and users of these solutions must have sufficient knowledge to properly interpret and evaluate for reliability the statements that such systems generate” (Regional administration). Other participants however mentioned that tests and experimentations were already ongoing for such systems: “Examples are available” (Private sector); “We have already had a test project” (Finances).

The third main topic of discussion concerned the actors involved in the development and implementation of these new tools. Some participants mentioned that feasibility largely depends on the nature of the involved actors, arguing that such tools are within the reach of some actors but not others. Others stressed that the development and implementation of these tools would not be possible without a collaboration between various actors: “The development of new tools that offer better traceability and experimentation will probably only be possible through the collaboration of several actors” (Private sector). They notably evoked the need for a collaboration between private and public actors: “Cross-fertilisation with specialists from the private market seems to me a logical approach to building the most declarative model” (Private sector).

The following figure presents a tag cloud that synthetizes the themes that were identified during the qualitative analysis of question 5.2.

Figure 29 - Tag cloud for question 5.2

QUESTION 5.3

The third question of the fifth section of the survey is as follows: To what extent would the increased explicability obtained by these new tools be compatible with the effectiveness in the fight against future fraud?

Qualitative analysis

A thematic analysis allowed to identify four main categories of answers to this question. First, a considerable number of participants stressed the necessity to find an equilibrium between the explicability of algorithms and their effectiveness in detecting fraud. Explaining how AI-assisted fraud decisions are reached is viewed as a necessity, including for fostering trust in those systems: "It is a necessity, as it is both ethically and legally difficult to leave fraud fighting to an AI algorithm that cannot be explained clearly" (Federal administration). Similarly, "If one suspects someone of fraud based on an AI system but cannot explain why himself, it is difficult to justify, especially if no fraud is found afterwards. This does not help confidence in such AI systems" (Private sector). However, the risk is that being too transparent might help fraudsters adapt to new fraud detection techniques: "Being careful not to pass on too much information that could deliberately leave one out of certain patterns" (Social security). Similarly, "if the analysis method is too clear it is easily possible to bypass it to avoid the detection of fraud" (Private sector). Thus, some participants argue that the degree of transparence regarding how the decision was reached should be dealt with caution and be subjected to a risk-benefit assessment: "A detailed analysis of the benefits/risks by the field actors is necessary to determine the level of explicability" (Not-for-profit organization). "This depends on who it is to be explained to. If it is only up to the judge in a lawsuit to prove that the algorithm used does not discriminate, there is no problem. If it also needs to be explained to the accused, this is more sensitive" (Social security).

Second, some participants argued that the increased explicability obtained via these new tools would probably not interfere with the effectiveness in the fight against future fraud. Although some conceded that this intuition would have to be confirmed by "further academic research" (Regional administration), participants also voiced their views on the positive effects of an improved explicability of tools on civil servants' work: "This is fully compatible. The use of these new tools will contribute to the more efficient use of control resources (e.g., social inspectors). They will have to spend less time on observations that are compliant with the regulations and will consequently be able to spend more time on observations that have a greater potential for non-compliance" (Social security).

Third, a few participants reasoned that the explicability of algorithms should perhaps receive less attention than improving their performance. In other words, these participants argued that, in some conditions, improving the effectiveness of new IT tools should be more important than improving their explicability: "it is not always necessary in my view, however, to be able to explain why a model makes a certain choice. I think that in that case it should be sufficient to look at the results of the model" (Finances). Similarly, "Everyone wants the development of AI-based IT tools to fight fraud, so what matters is the purpose, the fight against fraud" (Mutuality).

The fourth main topic concerns some other observations made by participants. Among those observations was the necessity to keep humans actively involved in the monitoring of fraud detection

processes that rely on AI. For instance, it was argued that an appeal should always allow for a manual examination of individual cases: “I think that the important thing with these new tools is also to have the possibility of an appeal and a manual analysis of the file. The tool, regardless of its analysis method, must make it possible to detect whether there is a possibility of fraud. A complementary analysis must then be done to confirm this fraud” (Private sector). Another observation is that explicability should conform to existing rules, including the GDPR: “Explainability should be about methodology and compliance with GDPR rules, not individual research files” (Social security). Finally, another observation was that new tools should bring a clear added value in order to be adopted: “Without clear added value, new tools should not be used” (Social security).

The following figure presents a tag cloud that synthetizes the themes that were identified during the qualitative analysis of question 5.3.

Figure 30 - Tag cloud for question 5.3

3.6. SECTION 6 - ENSURING THE LEGAL COMPLIANCE OF THE SYSTEM

The sixth section of the Delphi survey aimed at bringing some possible answers to the compatibility between the current legislation and the technological choices in the fight against fraud and to the difficulty of articulating complex legislations with the adoption of new IT tools in the fight against fraud. Based on the results of the previous steps of the DIGI4FED research project, a series of possible solutions were presented to the participants. The first solution consists in promoting the development of a legislation that is more compatible with the digital framework. The second solution consists in simplifying the task of privacy actors by adopting solutions and tools developed at the European level. The following text box presents the short background piece that was presented to the survey participants:

According to the workshops and the interviews, two issues raise questions about the **compatibility between the current legislation and the technological choices in the fight against fraud**. The first issue is the interpretation and implementation difficulties associated with the General Data Protection Regulation (GDPR). The lack of perceived clarity of the GDPR complicates the task of data privacy actors and leads to divergent interpretations between the data protection officers (DPOs) of the different administrations. Another issue is the **difficulty of articulating complex legislations with the adoption of new IT tools in the fight against fraud**. Existing legislation (on social and fiscal matters, public procurement rules, etc.) is sometimes unsuited to the integration of new digital tools.

The governance model could therefore ensure that the overall compatibility of the system with legislation is improved by:

- **Promoting the development of a legislation that is more compatible with the digital framework**. In addition to legal experts, the involvement of other experts (such as computer scientists) in the reflection process could help ensure that legal instruments are compatible with the new digital framework. The use of a regulatory sandbox mechanism could also help to develop and test different regulatory frameworks for the use of new technologies in the fight against fraud. However, there are still some unknowns as to the viability of this experimental approach to law.
- **Simplifying the task of privacy actors by adopting solutions and tools developed at the European level**. To strengthen the compatibility of the system with national legislation and the GDPR, it would be possible to rely on certain tools developed in compliance with EU ethical and regulatory standards (such as ESSIF and EBSI) for the construction of a data exchange platform. Such an approach could facilitate the interpretation of rules and decision-making by DPOs and other privacy actors (DPA, CSI). This could also contribute to the development of a national legislation on taxation and social security that is more compatible with the use of new technologies.

QUESTION 6.1

The first question of the sixth section of the survey is as follows: Do you think that the proposed solutions can provide a clear and understandable response to the challenges faced by DPOs? Could you specify why? Possible answers are: Yes; Partly; No; No opinion.

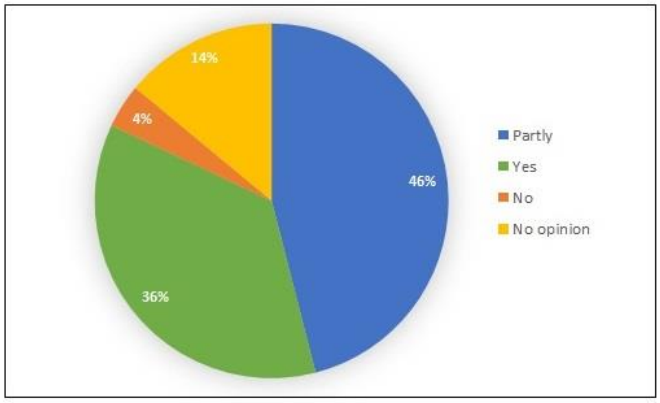
Short summary

A total of 28 participants answered this question. Overall, 36 % of participants agreed that the proposed solutions can provide a clear and understandable response to the challenges faced by DPOs. 46 % of participants only partially agreed that the proposed solutions can provide a clear and understandable answer and 4 % did not agree with this idea. 14 % had no opinion. The following figure synthetizes participants' answers to question 6.1.

Figure 31 - Question 6.1 summary: can these solutions provide a clear and understandable response to DPOs' challenges?

28 answers

e=Partly	13	46 %	
o=Yes	10	36 %	
p=No opinion	4	14 %	
n=No	1	4 %	



Qualitative analysis

In addition to these numbers, a thematic analysis of participants' supplementary answers allowed us to identify two key topics of discussion. The first main topic voiced by participants was the importance of adopting a clear and adequate legal framework so to facilitate the task of DPOs and the integration of new technologies in general. Some participants stressed the necessity to adapt and uniformise the current legal framework to ease DPOs' tasks: "The task of a DPO is to assess whether a processing or intended processing is in accordance with the current privacy guidelines and, if necessary, requires preventive adjustment; cf. the importance of (D)PIAs. A uniform framework would simplify this exercise and allow for a greater focus on the essence: assessing proportionality" (Finances). Similarly, the development of a clear and understandable legal framework was seen as a priority: "New legislative framework (adapted to GDPR) by e.g., allowing data exchange in certain explicitly mentioned situations is essential" (Social security). Other participants mentioned and agreed with the need for a re-connection between the legal framework and the current realities of IT developments: "Concerning the law, the drafting of laws should be less disconnected from IT but also from business. Sometimes, they are well written for IT but unmanageable to implement in the business" (Justice). Similarly, "The use of legislation that is 'designed for digital' should indeed make it easier to map notions and concepts from the legislation onto elements of the IT solution that implements this legislation and thus make it easier for the DPO to assess whether this IT solution meets the legal requirements of the GDPR" (Regional administration). These respondents tended to consider "the inclusion of more IT expertise in the legislative process around digitization as a win" (Federal Administration).

However, a few participants stressed that priority should be given to adapt new IT tools to the legal framework instead of adapting the legal framework to new IT developments: "In order to fight against fraud the legislators have determined tools (for which they must now provide the necessary means). The computer tool is an additional tool, not a replacement tool" (Union).

The second main topic voiced by participants concerned the advantages and the limits to the adoption of IT tools developed at the EU level. Participants mentioned the advantages of GDPR compliant tools in facilitating DPOs' tasks: "Indeed, the use of IT solutions developed at the European level that are already 'GDPR-proof' and 'AI-ethical' should make it easier for data protection officers and other

privacy actors to grant permission to deploy these IT solutions in a government context" (Regional administration); "Unity in interpretation of GDPR regulations can indeed be promoted by European instruments" (Social security). Other participants did, however, mention some limits to those tools. Some argued that IT and societal developments are constant and that it would likely prove difficult to continuously adapt such tools to new upcoming challenges: "These solutions will never be able to provide a complete and conclusive answer to the problems presented. The nature of the problems is ultimately, partly due to the constantly evolving society, that they evolve. As a result, continuous monitoring and evolution of enforcement and practical tools is needed" (Social security). Another position was that the adoption of new tools (including GDPR compliant tools) would probably help with some issues. However, these new tools would also inevitably bring new problems that will have to be dealt with: "GDPR is a solution to the privacy problem developed at the European level, but as indicated here, this creates new problems. Just as the European-level 'solutions' (ESSIF, EBSI) indicated here also create new problems in addition to solving a particular problem" (Federal administration).

The following figure presents a tag cloud that synthetizes the themes that were identified during the qualitative analysis of question 6.1.

Figure 32 - Tag cloud for question 6.1

QUESTION 6.2

The second question of the sixth section of the survey is as follows: Do you think that the proposed solutions can provide a sustainable response to the challenges faced by privacy actors? Could you specify why? Possible answers are: Yes; Partly; No; No opinion.

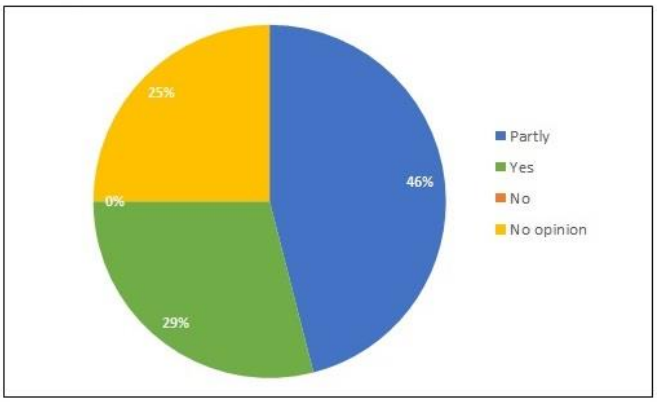
Short summary

A total of 28 participants answered this question. Overall, 29 % of participants agreed that proposed solutions can provide a sustainable response to the challenges faced by privacy actors. 46 % of participants only partially agreed with this idea. 25 % had no opinion. The following figure synthetizes participants' answers to question 6.2.

Figure 33 – Question 6.2 summary: can these solutions provide a sustainable response to privacy actors' challenges?

28 answers

e=Partly	13	46 %	
o=Yes	8	29 %	
p=No opinion	7	25 %	
n=No	0	0 %	



Qualitative analysis

In addition to these numbers, a thematic analysis of participants' supplementary answers allowed us to identify one main topic of discussion. The topic voiced by participant concerns the adaptability of our proposed solutions to new challenges. A concern was that technology evolves at such a rapid pace that new unforeseen challenges will likely arise: "New, currently unknown technological developments in areas such as IoT or metaverse will undoubtedly create new, additional privacy challenges that are not necessarily covered by the governance model proposed here" (Regional administration). To improve adaptability, some mentioned the necessity to speed-up the law creation process: "the process of drafting laws is accelerated (otherwise the technology is already outdated when the law comes out)" (Justice).

As for the previous question, some other participants mentioned the advantages and the problems associated with the adoption of new GDPR compliant IT tools. They also stressed the need for a clear and adequate legal framework.

The following figure presents a tag cloud that synthetizes the themes that were identified during the qualitative analysis of question 6.2.

Figure 34 - Tag cloud for question 6.2

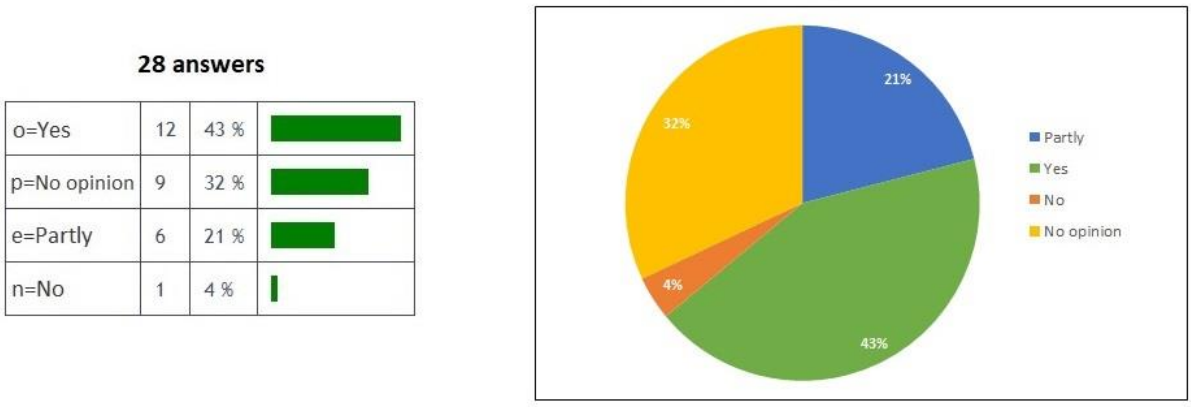
QUESTION 6.3

The third question of the sixth section of the survey is as follows: Do you think that these new approaches to law development (such as regulatory sandboxes) can be implemented? Could you specify why? Possible answers are: Yes; Partly; No; No opinion.

Short summary

A total of 28 participants answered this question. Overall, 43 % of participants agreed that new approaches to law development (such as regulatory sandboxes) can be implemented. 21 % of participants only partially agreed that new approaches to law can be implemented and 4 % did not agree with this idea. 32 % had no opinion. The following figure synthetizes participants' answers to question 6.3.

Figure 35 - Question 6.3 summary: can we implement these new approaches to law development?



28 answers

o=Yes	12	43 %	
p=No opinion	9	32 %	
e=Partly	6	21 %	
n=No	1	4 %	

Qualitative analysis

In addition to these numbers, a thematic analysis of participants' supplementary answers allowed us to identify two key topics of discussion. The first main topic voiced by participants is their opinion on regulatory sandbox approaches and their feasibility. Most participants agreed that regulatory sandboxes are a viable and innovative approach to better articulate the legal framework with the adoption of new IT tools in the fight against fraud: "Yes, and it is desirable. We sometimes see legislative changes that have come into force that include the creation of platforms to fight against this or that, but without any analysis, whether organizational or technical, being carried out in advance (no feasibility study or risk and opportunity analysis)" (Social security). Many considered this option as desirable: "Especially if legislation and new technological developments are developed simultaneously and iteratively with digital legislation also following a principle of public dev (pre-release) to public prod (release)" (Federal administration); "nice practical initiative" (Social security). Some did however stress the need for clear rules and guidelines surrounding the use regulatory sandboxes: "There is a need for clear guidelines on how such a regulatory sandbox should be set up and managed (how should public procurement for this take place, how should this be monitored and evaluated, etc.)" (Regional administration). A few did doubt the feasibility of such an approach: "I don't think it is currently legally possible (especially with the RGPD) but it would be to encourage" (Justice).

Respondents also voiced some other general concerns and caveats. As for the questions 6.1 and 6.2, participants voiced their concerns over the adaptability of our proposed solutions to new challenges. As mentioned in question 6.1, another position was that priority should be given to adapt new IT tools to the legal framework instead of adapting the legal framework to new IT developments: "Pilot projects can be inspiring, but the goal should never be to adapt a legislation with certain societal goals to "the digital framework. The digital framework should adapt to the societal objectives" (Social security).

The following figure presents a tag cloud that synthetizes the themes that were identified during the qualitative analysis of question 6.3.

Figure 36 - Tag cloud for question 6.3

3.7. ADDITIONAL ELEMENTS

In addition to the previous questions, the last section of the questionnaire offered to participants the opportunity to express their general impressions and observations. More specifically, we asked participants if there were any other issues they would have liked to see mentioned in the survey. A thematic analysis of participants' answers allowed us to identify three main topics of discussion.

The first main topic brought by respondents was the importance of cooperation and inclusion of diverse groups of actors in the governance model. Some participants stressed that the integration of new technologies in the fight against fraud requires the mobilization and cooperation of various categories of public actors. The necessity of "getting people on board" (Private sector) is for instance applicable to the various levels of government in Belgium: "Increased cooperation in this area between the different levels of government in Belgium" (Social security). Others argued that the governance model should be more inclusive towards actors from the civil society and citizens in general. A greater involvement of these actors is essential since a successful adoption of new IT tools largely depends on their endorsement: "The proposed governance model must also provide room for interaction with and input from 'civil society', i.e., ordinary citizens must also be systematically involved (via the appropriate civil society organisations) in the further elaboration and operationalisation of the governance model. The citizen is ultimately the person who must have the last word" (Regional administration).

The second main topic voiced by participants was the importance of adequate rules and guidelines surrounding confidentiality and the independence of the services in charge of data governance. For instance, an opinion was that achieving an adequate protection of personal data should be a priority but that strict confidentiality rules should not impede fraud detection: "the fight against fraud in an interconnected and increasingly digital world seems to me essential. It must be guaranteed that these search and detection methods prevent access for other purposes. Finally, we must avoid that too strict confidentiality rules hinder the detection of fraud and protect the interest of fraudsters" (Mutuality).

Another concern was to set up the appropriate rules and guidelines to ensure the strict “independence of the federal services creating the new platforms” (Justice).

Finally, some participants brought to the fore the topic of skills and expertise. More specifically, these stakeholders argued that one of the key issues that should be better reflected and addressed in the proposed governance model is the IT skill shortage in the labour market: “I believe that an additional problem is the 'war for talent'. There is a strong growing demand for talent with knowledge of new technologies, implementation and related legal aspects. However, the supply of this talent on the labour market is not increasing along with the demand. Solutions and the problem itself are, in my opinion, not sufficiently reflected in the research presented” (Social security).

To conclude on a more general note, an open suggestion was to produce a new iteration of the governance model based on the data that we collected with this survey: “I think it would be good to have another iteration of discussion based on the input. I think the questionnaire risks freezing the discussion on the 'who' and 'how' when it should be defining the 'what'!” (Federal administration).

4. MODEL TESTING

As presented in the previous section, participants' answers were analyzed in several ways. First, simple descriptive statistics were performed based on participants' answers to the scale survey questions (where participants expressed their level of agreement about the feasibility, efficacy, simplicity, etc. of our proposed design solutions). The additional comments left by participants were then qualitatively analyzed so that this supplementary information can be used to improve, or reframe, our governance model.

Each of these survey questions can be linked to a specific evaluation criterion. A set of eight evaluation criteria were specifically selected (see D3.3.) with the purpose of testing the validity of our design artefact. The following table synthesizes the correspondence between the survey dimensions, the survey questions, and the associated evaluation criteria.

Survey dimensions, questions, and corresponding evaluation criteria

Survey dimension	Question and evaluation criteria
A. Fostering citizen trust	Question 1.1: Overall efficacy Question 1.2: Overall suitability Question 1.3: Overall suitability
B. Promoting coordination and interoperability between administrations	Question 2.1: Open-ended question Question 2.2: Overall efficacy Question 2.3: Feasibility Question 2.4: Open-ended question
C. Limiting public actors' dependence towards private actors	Question 3.1: Overall efficacy Question 3.2: Open-ended question Question 3.3: Feasibility
D. Values and data governance	Question 4.1: Overall suitability Question 4.2: Sustainability Question 4.3: Overall simplicity Question 4.4: Cognitive aspects
E. Improving the explainability of the analysis process	Question 5.1: Overall efficacy Question 5.2: Feasibility Question 5.3: Sustainability
F. Ensuring the legal compliance of the system	Question 6.1: Overall simplicity Question 6.2: Sustainability Question 6.3: Feasibility

In order to test our model, we applied a 65% benchmark for each criterion. We consider that our design artefact respects a given criterion if 65% of participants either agree, or partially agree in their answers to all the questions pertaining to a given evaluation criterion.

Two evaluation criteria were not addressed by dedicated questions (stakeholder endorsement and overall consistency). Instead, these criteria were assessed with the help of a thematic analysis of participants' full set of answers across the survey questions. Open coding was used to assess and rate participants' endorsement of the model and their perception of the model's consistency. The open-ended questions of the survey (question 2.1; question 2.4; and question 3.2) were qualitatively analyzed using a thematic analysis. However, we did not rely on these questions to test our design artefact. Instead, the qualitative analysis of participants' answers to these specific questions will primarily serve the purpose of providing useful additional information to refine, or revise, our governance model.

4.1. OVERALL EFFICACY

The overall efficacy criterion assesses if the proposed governance model is perceived as an effective and efficient solution for the integration of new technologies in the fight against tax fraud and social security infringements. In our Delphi survey, four questions did specifically address the efficacy of the solutions that are proposed in our design artefact. These questions are the following:

- Question 1.1: Do you think that such solutions can provide an effective response to the lack of trust among citizens?
- Question 2.2: Do you think that the proposed solutions could help overcome this obstacle?
- Question 3.1: Which of the following statements best illustrates your view regarding the proposed solutions to limit the dependence of public actors towards private actors?
- Question 5.1: Do you think that the proposed solutions can improve the explainability of decisions based on AI?

We opted for a 65% benchmark to assess our design artefact based on this criterion. In other words, if at least 65 % of participants either agree, or partially agree in their answers to the aforementioned questions, we would consider that our design artefact meets the efficacy criterion.

A short analysis indicates that, on average, 32 % of participants agree that the proposed design is effective for the integration of new technologies in the fight against tax fraud and social security infringements. 52 % of participants partially agree with this idea, while 12.8 % disagree with it. 3.2 % have no opinion. More specifically, for each question:

- Question 1.1: 17 % agree; 67 % partially agree; 14 % disagree; 1 % no opinion
- Question 2.2: 38 % agree; 44 % partially agree; 19 % disagree
- Question 3.1: 16 % agree; 61 % partially agree; 10 % disagree; 6 % no opinion
- Question 5.1: 61 % agree; 29 % partially agree; 7 % disagree; 4 % no opinion

On average, 84 % of participants either agree, or partially agree with the effectiveness of the design. This result indicates that our design artifact meets the efficacy criterion. However, due to the large proportion of participants indicating that they only partially agree with the question statements, we strongly suggest that any further adaptations to our model should take into consideration the results of the qualitative analysis of participants' answers to these questions. This is particularly the case for question 1.1 (67 % partially agree) and question 3.1 (61 % partially agree).

Considering question 1.1, the qualitative analysis results stressed that a considerable number of participants did express some concerns regarding the ability of the model to propose an effective response to the lack of trust among citizens. Five main concerns were voiced by participants:

- First, although some participants expressed their agreement with a decentralized approach to data management, many expressed their scepticism to this approach. Some expressed a lack of confidence in this technical solution while others argued that decentralized solutions might appear too complex and abstract to generate trust among citizens: “I think it is a very relevant tool, but it will not be a tool for improving citizen trust. These concepts are far too abstract for the average citizen” (Social security).
- Second, although many participants saw in a positive light the potential gains in transparency and trust brought by digital wallet solutions, a few participants did consider that the model should go one step further by providing full transparency to citizens as well as the ability to fully control and manage their personal data. A considerable number of participants also pointed out the limits of digital wallets solutions. Indeed, some argued that digital wallets would not necessarily foster trust among citizens if they are not convinced with the good intentions of those who are issuing and managing these wallets. Other participants stressed that citizens’ ability to control their data should remain somewhat limited, especially when it comes to granting access to some of their data to public authorities: “there are surely a lot of government linkages to the data that would be non-optional” (Scholar).
- The third concern voiced by participants was the nature of citizens’ trust itself. A significant number of participants stressed that the proposed design solutions would probably not greatly improve citizens’ trust regarding the use of their personal data by public authorities because the main underlying issue remains citizens’ mistrust of public authorities in general: “It is not so much the tool that has been put in place as the people who manage the tool that scares and loses the trust of the citizen. The citizen is ready to reveal personal data for a TV game show but will hesitate for the state because he is afraid of what the latter could do with the information” (Private Sector).
- The fourth concern brought by stakeholders was the importance of communication with citizens. Some stakeholders mentioned that new tools and technical solutions (such as digital wallets) might not suffice to foster trust as long as a good communication with citizens is lacking.
- Finally, the fifth concern expressed by stakeholders was the level of IT related skills among citizens. Some participants were concerned that the proposed solutions would prove too complex or not user friendly enough for citizens. The risk is that the proposed solutions (decentralization and digital wallets) would further exclude those who are already affected by the digital divide.

Considering question 3.1, the qualitative analysis results stressed that many participants considered that the proposed model solutions would only be partially effective in limiting the dependence of public actors. Three main concerns were voiced by participants:

- The first concern was the necessity to acknowledge the pivotal role and importance of private IT solutions providers in relation with the public sector. Many stakeholders argued that the involvement of private actors remains and will remain necessary and/or inevitable. Some mentioned the important financial resources at the disposal of some private actors (in contrast

with public actors who struggle to internalize competences and to maintain job attractiveness): "Internalization requires budget: it means attracting employees in competition with the private sector and is at odds with personnel savings in the government, which then has no choice but to work with external parties" (Federal Administration). Others mentioned that, even if measures are taken to internalize competences, a dependence to private technological solutions will remain "for certain niche solutions" (Social security). Several participants also affirmed that they tend to consider private IT solution providers as generally more competent and reliable than public actors, including on the topics of data security and personal data protection. In this view, many considered that some private IT solution providers have gained such a technological edge that it would be difficult for national or European players to compete with them. Given these elements, several stakeholders strongly advocated for a collaboration between private and public actors.

- A second concern expressed by participants was that a fully independent public sector might jeopardize the collaboration with the private sector. Indeed, they argued that bolstering in house projects and the internalization of expertise would encourage the self-centeredness of the public sector and an increased dependence on a limited number of internal bodies. As such, the adoption of open standards and technologies was seen as a way to reduce dependence while maintaining a form of collaboration with private actors.
- The third main concern brought by participants concerns the obstacles that are faced by the public sector in achieving a reduction of its dependence towards private actors. According to participants, the most important obstacle is the lack of internal skills and expertise. This lack of expertise was also closely associated with the lack of resources within the public sector. According to stakeholders, limited resources negatively affect administrations' ability to maintain job attractiveness and internalize IT expertise: "It will not be possible to internalize this at FPS BOSA either, unless there are more flexible working conditions there (higher pay, flexible hours, fringe benefits, etc.)" (Finances). Some participants suggested to resort to alternate IT solutions to limit the dependance towards private actors. Such solutions included IT solutions developed by European actors and open-source solutions.

The full results of our thematic analysis of participants' answers to questions 1.1; 2.2; 3.1; and 5.1 are presented in section 3.1; section 3.2; section 3.3; and section 3.5.

4.2. OVERALL SUITABILITY

The overall suitability criterion assesses if the proposed governance model is perceived as a useful and relevant solution for the integration of new technologies in the fight against tax fraud and social security infringements. In our Delphi survey, three questions did specifically address the suitability of the solutions that are proposed in our design artefact. These questions are the following:

- Question 1.2: Do you think that the generalization of a digital wallet system could be an adequate solution to a lack of citizen trust?
- Question 1.3: Do you think that a decentralized data management could be an appropriate response to a lack of citizen trust?
- Question 4.1: Do you think it is relevant that the public managers should endorse the role of key regulators in data governance?

We opted for a 65% benchmark to assess our design artefact based on this criterion. In other words, if at least 65 % of participants either agree, or partially agree in their answers to the aforementioned questions, we would consider that our design artefact meets the suitability criterion.

A short analysis indicates that, on average, 29.5 % of participants agree that the proposed design is suitable considering the integration of new technologies in the fight against tax fraud and social security infringements. 47.4 % of participants partially agree with this idea, while 15.8 % disagree with it. 7.3 % have no opinion. More specifically, for each question:

- Question 1.2: 19 % agree; 59 % partially agree; 19 % disagree; 3 % no opinion
- Question 1.3: 18 % agree; 59 % partially agree; 21 % disagree; 3 % no opinion
- Question 4.1: 55 % agree; 21 % partially agree; 7 % disagree; 17 % no opinion

On average, 76.9 % of participants either agree, or partially agree with the suitability of the design. This result indicates that our design artifact meets the suitability criterion. However, due to the large proportion of participants indicating that they only partially agree with the question statements, we strongly suggest that any further adaptations to our model should take into consideration the results of the qualitative analysis of participants' answers to these questions. This is particularly the case for question 1.2 (59 % partially agree). A similar attention should also be given to the qualitative analysis results for question 1.3 (59 % partially agree) which also presents a high percentage of participants who disagree (21 %) with the suitability of decentralized data management solutions in fostering citizen trust.

Considering question 1.2, the qualitative analysis results stressed that a considerable number of participants did express some concerns regarding the suitability of a generalization of digital wallet systems in fostering citizen trust. Five main concerns were voiced by participants:

- First, although many tended to approve the potential gains in control and transparency brought by digital wallet solutions, some stakeholders mentioned that digital wallets solutions should go one step further by providing full transparency to citizens as well as the ability to fully control and manage their personal data. A significant number of participants also pointed out the limitations of digital wallet solutions in fostering trust among citizens. They argued that digital wallets would not necessarily help fostering trust if citizens are not convinced with the good intentions of those who are issuing and managing these wallets: "This solution is not a magic tool to gain trust and can have the opposite effect (feeling that the government is collecting a lot of data on its citizens)" (Not-for-profit organization). Other participants stressed that citizens' ability to control their data should remain somewhat limited, especially when it comes to granting access to their data to public authorities.
- As for question 1.1, another main concern voiced by participants was that digital wallet solutions would probably not greatly improve citizens' trust regarding the use of their personal data by public authorities because the main underlying issue remains citizens' mistrust of public authorities in general "For a part of the citizens, such digital wallets will give the impression that the government wants to gain more control over them instead of the other way around" (Federal Administration).

- The third concern voiced by participants was the lack of proper communication with citizens regarding these digital wallets. Indeed, a significant number of stakeholders stressed that digital wallets might not suffice to foster trust if they are not accompanied by effective communication efforts from public authorities. It is important to make sure that the added value and the "benefit for the citizen in terms of services must be made obvious" (Not-for-profit organization) and communication efforts might help on this aspect.
- The fourth main concern expressed by participants was the issue of digital divide and the level of IT related skills among citizens. Stakeholders were concerned that digital wallet solutions would become a hinderance for some citizens and small businesses due to their complexity and their lack of user-friendliness. The risk is thus to "lose sight of the people who are not "on board" with digitalization" (Social security). However, one solution to remedy this issue would be through adequate communication and education.
- The fifth and final concern brought by stakeholders considers the possible technical issues associated with digital wallet solutions. One of such potential issues is security as some argue that the multiplication of wallets (with different issuers) could lead to security risks.

Considering question 1.3, the qualitative analysis results stressed that a considerable number of participants did express some concerns regarding the suitability of a decentralized approach to data management in fostering citizen trust. Three main concerns were voiced by participants:

- First, and as for question 1.1, a main concern voiced by stakeholders concerned the proclaimed added-value and benefits of decentralization. Although a number of participants argued in favour of decentralization, many also expressed some criticism towards this approach. Some stated that they were not convinced that decentralization could generate trust among citizens: "Decentralized means that data is distributed to multiple parties. This creates distrust" (Social security). Others considered decentralization as too complex and abstract to generate trust among citizens: decentralization is "not visible and too abstract for the citizens. Even if it does in fact contribute to this, the average citizen cannot understand that this action is done for this purpose and does not see the results (not tangible for him)" (Justice). Some participants also questioned the relevance of a decentralized approach given that the use case remains unclear to them. In addition to the relevance of this approach, others questioned the lack of hindsight regarding decentralized solutions, such as blockchain.
- The second main concern brought by participants was the lack of proper communication with citizens. Some stakeholders argued that privileging a decentralized approach to data management might not suffice to foster citizen trust without appropriate communication efforts from public authorities: "For trust, however, one must explain to the citizen what exactly decentralized data management means" (Finances).
- Finally, a third concern voiced by participants relates to use of data by public authorities. Some argued that in order to improve trust among citizens, public authorities should consider minimizing their general use of citizen data instead of adopting new tools and technical solutions.

The full results of our thematic analysis of participants' answers to questions 1.2; 1.3; and 4.1 are presented in section 3.1; and section 3.4.

4.3. FEASIBILITY

The feasibility criterion assesses if the design solutions of the proposed governance model can be considered feasible on a political / financial / technological / legal level. In our Delphi survey, four questions did specifically address the feasibility of the solutions that are proposed in our design artefact. These questions are the following:

- Question 2.3: Do you think that such a data exchange platform between administrations is feasible (legally, organizationally, etc.)?
- Question 3.3: Do you think that a federal service would be able to assume the development and the technical management of a new data exchange platform?
- Question 5.2: Do you think that the development and implementation of these new, explainable, tools is within the reach of the different actors involved?
- Question 6.3: Do you think that these new approaches to law development (such as regulatory sandboxes) can be implemented?

We opted for a 65% benchmark to assess our design artefact based on this criterion. In other words, if at least 65 % of participants either agree, or partially agree in their answers to the aforementioned questions, we would consider that our design artefact meets the feasibility criterion.

A short analysis indicates that, on average, 43.2 % of participants agree that the proposed design is feasible considering the integration of new technologies in the fight against tax fraud and social security infringements. 38.1 % of participants partially agree with this idea, while 5.1 % disagree with it. 13.6 % have no opinion. More specifically, for each question:

- Question 2.3: 50 % agree; 40 % partially agree; 3 % disagree; 7 % no opinion
- Question 3.3: 44 % agree; 50 % partially agree; 3 % disagree; 3 % no opinion
- Question 5.2: 36 % agree; 39 % partially agree; 11 % disagree; 14 % no opinion
- Question 6.3: 43 % agree; 21 % partially agree; 4 % disagree; 32 % no opinion

On average, 81.3 % of participants either agree, or partially agree with the feasibility of the design. This result indicates that our design artifact meets the efficacy criterion. However, due to the large proportion of participants indicating that they only partially agree with the question statements, we strongly suggest that any further adaptations to our model should take into consideration the results of the qualitative analysis of participants' answers to these questions. This is particularly the case for question 3.3 (50 % partially agree). A similar attention should also be given to the qualitative analysis results for question 6.3, which presents a high percentage of participants with no opinion (32 %).

Considering question 3.3, the qualitative analysis results stressed that a considerable number of participants did express some concerns regarding the feasibility of a federal service assuming the development and the technical management of a new data exchange platform. Three main concerns were voiced by participants:

- The first concern voiced by several respondents was that the development and the technical management of a new data exchange platform appears to be fully entrusted to public authorities.

Instead, many stakeholders agreed that federal services should work in collaboration with the private sector which can provide much-needed expertise and resources. In other words, these stakeholders suggested that public authorities should be "joining forces with a private partner where there is a lack of expertise" (Not-for-profit organization).

- The second concern brought by participants relates to the constraints that could negatively affect the development and subsequent management of such a platform by federal services. Among such constraints are the limited resources of the public sector as well as the lack of internal expertise. It was for example mentioned not to underestimate the costs and challenges associated with keeping the platform up-to date from a technical standpoint: "the problem of being able to stay up to date concerning technical evolutions is difficult to overcome in the administration (expenses and costs in training hours + daily work makes it quickly impossible to follow the evolutions)" (Justice). Some stakeholders also mentioned the lack of political will as a possible detrimental factor: "Politicians must want it and give real means to such a long-term project" (Social security).
- The third main concern, or observation, expressed by participants was the existence, within administrations, of systems that they consider close, or similar, to the proposed data exchange platform. Some stakeholders argued that the envisioned data exchange platform system already exists (at least partially) at the federal level. They notably stressed the existence of service integrators which already serve the purpose of facilitating the sharing of data between administrations at the federal level: "There is already a service integrator. The expectations should be specified and the BOSA service integrator should be used for example" (Federal administration).

The full results of our thematic analysis of participants' answers to questions 2.3; 3.3; 5.2; and 6.3 are presented in section 3.2; section 3.3; section 3.5; and section 3.6.

4.4. STAKEHOLDER ENDORSEMENT

The stakeholder endorsement criterion assesses if stakeholders agree with and trust the design solutions of the proposed governance model and if they are satisfied with the outcomes. In our Delphi survey, no question did specifically address the stakeholder endorsement for our design artefact. Instead, this criterion was assessed via a thematic analysis of each participant's full set of answers. Open coding was then used to assess each participant's endorsement of the model. The codes were used as follows: endorses; partly endorses; does not endorse; no position. We opted for a 65% benchmark to assess our design artefact based on this criterion. In other words, if at least 65 % of participants either endorse, or partially endorse the model in their full set of answers, we would consider that our design artefact meets the stakeholder endorsement criterion.

The analysis indicates that 28.6 % of participants did endorse the proposed design artefact for the integration of new technologies in the fight against tax fraud and social security infringements. 45.7 % of participants did partially endorse the model, 17.1 % did not endorse it, and 8.6 % had no clear position. On average, 74.3 % of participants either endorse, or partially endorse the design. This result indicates that our design artifact meets the stakeholder endorsement criterion. That being said, a large proportion of participants (45.7 %) indicated that they only partially endorse the model. Hence, we

strongly suggest that any further adaptations to our model should take into consideration the results of the qualitative analysis of participants' answers to the questionnaire.

On the one hand, the participants who endorsed the model praised several of its aspects such as its ability, or intent, to limit administration's dependence towards private IT solutions providers:

> "By doing this, we would promote internal knowledge and limit dependency" (Finances); "Yes, it is really necessary to reduce the dependence towards private actors because: each adaptation of the tool often requires the use of the firm that developed it; the security of the data can raise questions (for example the use of cloud solutions from an extra-european firm)." (Finances)

Some also voiced their agreement at the idea of giving citizens the ability to control and monitor their data with the help of digital wallets:

> "The positive effect lies in the empowerment one gives to the citizens who consider this important. On the other hand, one should not lose sight of the people who are not "along" with digitalization" (Social Security)

On the other hand, the participants who were less inclined to endorse the overall model did criticize several aspects of the model, such as its ability to provide definitive and durable answers to the identified problems:

> "These solutions will never be able to provide a complete and conclusive answer to the problems presented. The nature of the problems is ultimately, partly due to the constantly evolving society, that they evolve. As a result, continuous monitoring and evolution of enforcement and practical tools is needed" (Private sector)

Some also criticized the necessity to tackle public actors' dependance towards private IT solution contractors:

> "For my part, this is a false debate! The problem does not come from private actors. Private actors are often much more concerned about respecting the private data of their customers and in this case citizens than public actors themselves. For me the debate is about the competence of the different actors and especially about the respect by the business of data security constraints." (Private sector)

Others were less confident regarding the appropriateness of giving to citizens the ability to monitor and control the access to their personal data (with the help of digital wallet solutions):

> "It is legitimate to want to make sure that the citizen can better manage and control his personal data. However, the citizen should not necessarily have the choice to share or not his data with the administrations (e.g.: e-health platform, it is not up to the citizen to determine if doctors should be informed or not of medical history)." (Social Security)

4.5. COGNITIVE ASPECTS

The cognitive criterion assesses if the proposed governance model promotes knowledge and information exchange among stakeholders and if it fosters cognitive learning about the policy and its implications. In our Delphi survey, one question did specifically address the cognitive aspects in our design artefact. This question is as follows:

- Question 4.4: Do you think that better communication about the use of new technologies in the fight against fraud could lead to a better understanding and acceptance of these tools by citizens and companies?

We opted for a 65% benchmark to assess our design artefact based on this criterion. In other words, if at least 65 % of participants either agree, or partially agree in their answers to the aforementioned question, we would consider that our design artefact meets the cognitive criterion.

A short analysis indicates that 57 % of participants agree that the proposed design fosters cognitive learning and promotes knowledge and information exchange among stakeholders. While 21 % partially agree with this idea, 14 % disagree with it and 7 % have no opinion.

On average, 78 % of participants either agree, or partially agree regarding the ability of the design to foster cognitive learning and knowledge exchange. This result indicates that our design artifact meets the cognitive criterion. Although a large proportion of participants either agree or partially agree with the question 4.4 statement, we still consider relevant to consider the results of the qualitative analysis of participants' answers to this question. Further adaptations to our model could benefit from the additional insights brought by participants on that matter. The results of our thematic analysis of participants' answers to question 4.4 are presented in section 3.4.

4.6. OVERALL CONSISTENCY

The overall consistency criterion assesses if the proposed governance model is perceived as coherent, consistent, and sufficiently detailed. In our Delphi survey, no question did specifically address the overall consistency of the design artefact. Instead, this criterion was assessed via a thematic analysis of each participant's full set of answers. Open coding was then used to assess each participant's perception of the consistency of the model. The codes were used as follows: consistent; partly consistent; not consistent; no position. We opted for a 65% benchmark to assess our design artefact based on this criterion. In other words, if at least 65 % of participants either endorse, or partially endorse the model in their full set of answers, we would consider that our design artefact meets the overall consistency criterion.

The analysis indicates that 17.1 % of participants did consider that the proposed design artefact as generally consistent. 65.7 % of participants considered the model as partially consistent, while 8.6 % did not consider it consistent. 8.6 % had no clear position. On average, 82.8 % of participants either agree, or partially agree upon the overall consistency of the design. This result indicates that our design artifact meets the consistency criterion. That being said, a large proportion of participants indicated that they consider the model only partly consistent. Hence, we strongly suggest that any further adaptations to our model should take into consideration the results of the qualitative analysis of participants' answers to the questionnaire.

The participants who considered the model as partly consistent (65.7 %) noted that the model lacked several aspects that they considered fundamental considering the general orientation of the model. For instance, although the governance model intends to improve citizens' control over their personal data, some participants noted the limited space given to civil society representatives in the proposed design:

> "The proposed governance model must also provide room for interaction with and input from 'civic society', i.e. ordinary citizens must also be systematically involved (through the appropriate civil society organizations)

> in the further elaboration and operationalization of the governance model. The citizen is ultimately the person who must have the last word" (Regional administration)

Similarly, some participants noted that we are unsure if citizens are really expecting some of the proposed design solutions (such as digital wallets):

> "Again: in all discussions around managing personal data and putting the responsibility for that on the citizen who has to manage it and give consent, the assumption is too much that the citizen is waiting for that." (Federal administration)

Others noted that the proposed model tends to put too much emphasis on technical solutions to identified problems rather than on legal aspects. Some consider that the model appears more concerned with the adaptation of the legal framework to new technologies when it should instead try to make new the IT solutions fit with the requirements of an updated legal framework.

> "Transformation is not just about data and IT, it's also about infrastructure, getting people on board and changing laws and regulations so that it becomes an enabler" (Private sector)

> "We need a legal framework. It is necessary and even essential." "In this legislative framework, it must be clearly stated that each individual is the owner of his or her data and that this data will be treated in accordance with the right to property and privacy. In order to fight against fraud, the legislators have determined tools (for which they must now provide the necessary means). The computer tool is an additional tool, not a replacement tool. It would be a real democratic danger if a machine, in the service of some, could analyze the data of everybody, indiscriminately and without limits." (Union)

4.7. OVERALL SIMPLICITY

The overall simplicity criterion assesses if the proposed governance model is considered simple enough to be understandable and accessible by stakeholders. In our Delphi survey, two questions did specifically address the simplicity of the solutions that are proposed in our design artefact. These questions are the following:

- Question 4.3: Do you think that the proposed solutions allow for a governance of data that can be understood by all actors concerned by the protection of personal data?
- Question 6.1: Do you think that the proposed solutions can provide a clear and understandable response to the challenges faced by DPOs?

We opted for a 65% benchmark to assess our design artefact based on this criterion. In other words, if at least 65 % of participants either agree, or partially agree in their answers to the aforementioned questions, we would consider that our design artefact meets the simplicity criterion.

A short analysis indicates that, on average, 27.3 % of participants agree that the proposed design is simple enough considering the integration of new technologies in the fight against tax fraud and social security infringements while 41.8 % partially agree with this idea. 12.7 % disagree with the simplicity of our design while 18.2 % have no opinion. More specifically, for each question:

- Question 4.3: 19 % agree; 37 % partially agree; 22 % disagree; 22 % no opinion
- Question 6.1: 36 % agree; 46 % partially agree; 4 % disagree; 14 % no opinion

On average, 69.1 % of participants either agree, or partially agree regarding the simplicity of the design. This result indicates that our design artifact meets the simplicity criterion. However, due to

the large proportion of participants indicating that they only partially agree or even disagree with the question statements, we strongly suggest that any further adaptations to our model should take into consideration the results of the qualitative analysis of participants' answers to these questions. This is particularly the case regarding participants' answers to question 4.3. Indeed, only 37 % of participants partially agreed with the simplicity of the design, 22 % disagreed with it, and 22 % had no opinion.

Considering question 4.3, the qualitative analysis results stressed that a considerable number of participants did express some concerns regarding the understandability of the proposed data governance for all the actors concerned by the protection of personal data. Four main concerns were voiced by participants:

- The first concern brought by participants was the need for a transparent and effective communication with citizens. Some stakeholders argued that, in order to achieve a clear and understandable data-governance, improved communication efforts are needed to explain to citizens how their data is handled by public authorities and for what purposes: "improving communication on data use is a way to give citizens and businesses more confidence in how their (personal) data are used (for fraud prevention)" (Regional administration). Some stakeholders also stressed the need for transparent communication, considering that citizens should be clearly and precisely informed on who uses their data, how, and with what purposes.
- The second main concern expressed by participants was the need for a clear legal framework and procedures to allow for an understandable data governance: "this must be analysed in depth and a whole series of guarantees, safeguards, procedures, etc. must be provided for" (Justice).
- The third concern brought by stakeholders was the limited involvement of citizens in the proposed data governance model. According to some stakeholders, citizens and businesses should also be actively associated to the construction of the governance model: "The first actors concerned by the protection of personal data are the citizens/businesses. They must have an active role in defining a governance model" (Not-for-profit organization).
- The fourth concern relates to relative complexity of the model. Some participants argued that the model needs to be kept simple to ease comprehension. In their view, complex solutions are often less accepted than simple ones.

The full results of our thematic analysis of participants' answers to questions 4.3 and 6.1 are presented in section 3.4; and section 3.6.

4.8. SUSTAINABILITY

The sustainability criterion assesses if the proposed governance model is resilient to changes and unforeseen events and if it can adapt and evolve in response to future challenges. In our Delphi survey, three questions did specifically address the model sustainability. These questions are the following:

- Question 4.2: Do you think that a (supervised) contribution from private actors could help administrations to adapt and maintain their fraud detection capacities?
- Question 5.3: To what extent would the increased explicability obtained by these new tools be compatible with the effectiveness in the fight against future fraud?

- Question 6.2: Do you think that the proposed solutions can provide a sustainable response to the challenges faced by privacy actors?

We opted for a 65% benchmark to assess our design artefact based on this criterion. In other words, if at least 65 % of participants either agree, or partially agree in their answers to the aforementioned questions, we would consider that our design artefact meets the sustainability criterion.

A short analysis indicates that, on average, 42.7 % of participants agree that the proposed design provides sustainable solutions considering the integration of new technologies in the fight against tax fraud and social security infringements. 38.7 % of participants partially agree with this idea, while 6.6 % disagree, and 12 % have no opinion. More specifically, for each question:

- Question 4.2: 59 % agree; 21 % partially agree; 14 % disagree; 7 % no opinion
- Question 5.3: 39 % agree; 55.5 % partially agree; 5.5 % disagree
- Question 6.2: 29 % agree; 46 % partially agree; 25 % no opinion

On average, 81.4 % of participants either agree, or partially agree regarding the sustainability of the design. This result indicates that our design artifact meets the sustainability criterion. However, due to the large proportion of participants indicating that they only partially agree with the question statements, we strongly suggest that any further adaptations to our model should take into consideration the results of the qualitative analysis of participants' answers to these questions. This is particularly the case regarding participants' answers to questions 5.3 (55.5 % partially agree) and 6.2 (46 % partially agree). A considerable number of participants also had no opinion (22 %) regarding the question 6.2.

Considering question 5.3, the qualitative analysis results stressed that a considerable number of participants did express some concerns regarding the sustainability of fraud fighting effectiveness given the increased explicability of new fraud detection tools. Three main concerns and observations were voiced by participants:

- First, many stakeholders highlighted the necessity to find an equilibrium between explicability of algorithms and their effectiveness in detecting fraud. Explaining how AI-assisted fraud decisions are reached was often viewed as a necessity. However, the risk is that being too transparent might help fraudsters adapt to new fraud detection techniques: "Being careful not to pass on too much information that could deliberately leave one out of certain patterns" (Social security). As a result, some stakeholders argued that the degree of transparence regarding how the decision was reached should be dealt with caution and be subjected to a risk-benefit assessment: "A detailed analysis of the benefits/risks by the field actors is necessary to determine the level of explicability" (Not-for-profit organization).
- A second concern voiced by a few participants was that the explicability of algorithms should perhaps receive less attention than improving their performance. These stakeholders argued that, in some conditions, improving the effectiveness of new IT tools should be more important than improving their explicability: "it is not always necessary in my view, however, to be able to explain why a model makes a certain choice. I think that in that case it should be sufficient to look at the results of the model" (Finances).

- A third observation brought by respondents was the necessity to keep humans actively involved in the monitoring of fraud detection processes that rely on AI. It was for instance argued that an appeal should always allow for a manual examination of individual cases: “I think that the important thing with these new tools is also to have the possibility of an appeal and a manual analysis of the file” (Private sector).

Considering question 6.2, the qualitative analysis results stressed that a considerable number of participants did express some concerns regarding the sustainability of our proposed solutions regarding the challenges faced by privacy actors (DPOs, etc.). One main concern was voiced by participants:

This concern relates to the adaptability of our proposed solutions to new challenges. Some participants argued that technology evolves at such a rapid pace that new unforeseen challenges will likely arise soon: “New, currently unknown technological developments in areas such as IoT or metaverse will undoubtedly create new, additional privacy challenges that are not necessarily covered by the governance model proposed here” (Regional administration). According to some participants, speeding-up the law creation process would perhaps mitigate this issue.

The full results of our thematic analysis of participants’ answers to questions 4.2; 5.3; and 6.2 are presented in section 3.4; section 3.5; and section 3.6.

5. GENERAL SYNTHESIS AND CONCLUSION

We conclude this deliverable with a summary of the main results brought by the qualitative analysis of the collected data, an overview of the model testing results, and a general conclusion regarding the objectives of the present contribution.

SYNTHESIS OF THE MAIN RESULTS OF THE SURVEY

The analysis results presented in section 3 were delivered for each separate survey question. This was done to provide a detailed account of participants' reactions, concerns, and arguments for each specific aspect of our proposed governance model. This was also done in view of facilitating model testing. However, at this point, we consider important to provide the reader with a more general overview of the results of a thematic analysis of participants' answers to the survey. Seven main categories of results can be highlighted following a general analysis of the collected data:

The first main category of results concerns stakeholders' general reflections about the needs and struggles of citizens regarding public authorities' use of their personal data. Many participants stressed the necessity to improve public authorities' communication efforts towards citizens. Adequate communication was often presented as an effective way to foster trust and acceptance among citizens and businesses: "better communication has only advantages. It will therefore certainly lead to a better understanding and more support among private actors" (Social security). Indeed, fostering citizens' trust was considered as a challenging task that would not be easily addressed with the help of technical solutions such as digital wallets and a decentralized approach to data management. According to a significant number of participants, adopting new tools or a new data management approach would have a limited impact on citizens' trust in public authorities using their personal data because the main underlying is rooted citizens' mistrust of public authorities in general: "It is not so much the tool that has been put in place as the people who manage the tool that scares and loses the trust of the citizen" (Private sector). Hence, to rebuild citizens' trust in public authorities, stakeholders insisted on making proper communication efforts towards citizens regarding the purpose of data use. To that end, participants did put the accent on transparency and explicability: "Transparency is essential in creating trust among citizens" (Federal administration). Stakeholders also insisted on the necessity to better communicate on the intentions and added value of the new IT tools that are being adopted by public authorities to combat fraud or to help citizens manage their personal data. For instance, although it was generally agreed that the improvements in personal data control and transparency brought by digital wallet solutions could theoretically contribute to trust, many argued that such trust gains would not be reached without proper communication over the purpose and added value of digital wallets. Indeed, many argued that digital wallets would not necessarily help fostering trust among citizens if citizens are not convinced with the good intentions of those who are issuing and managing wallets.

Besides the considerations on citizens' trust and communication efforts, many stakeholders stressed the necessity to consider the lack of IT expertise in the population. As such, the digital divide was presented as a concern that needs to be addressed when developing new tools that are destined for citizens' personal use (such as digital wallets). For instance, many stakeholders stressed that digital wallet solutions might prove too complex and not user-friendly enough for a wide adoption by citizens:

"to this day, there are those who do not yet have a bank card. They are still far away from digital wallets. The generalization of such a system will take years (maybe decades)" (Finances). Some participants also viewed the limited IT expertise of the population as an issue for the adoption of decentralized approaches to data management, which they considered too complex and abstract for most citizens. A few stakeholders also argued that this general lack of IT expertise would probably hinder the effects of any communication and transparency efforts made by public authorities because comprehension would remain limited among citizens.

The second main category of results covers the relationship between private and public actors. A significant number of participants saw the involvement of private actors in the digital transition of administrations as unavoidable. This was for many reasons. Some mentioned the important resources at the disposal of private actors. This contrasts with administrations who struggle to internalize expertise and maintain job attractiveness due to budget limitations. Others argued that a deep dependence to private technological solutions would always remain because of technological legacies in administrations, training requirements, and the inevitable need for "certain niche solutions" (Social security). Many stakeholders also considered that private IT solution providers tend to have a superior technical expertise and that it would prove difficult for competitive national or in house solutions to emerge. It was even argued that private IT solution providers tend to be more competent and reliable than public actors, including on the topics of data security and personal data protection: "Private actors are often much more concerned about respecting the private data of their clients, and in this case the citizens, than the public actors themselves. For me, the debate is about the competence of the different actors" (Private sector).

Such arguments may explain why a considerable number of stakeholders did argue in favour of a collaboration between private and public actors: "Digital expertise is scarce in the marketplace, so partnering with the private sector is evident. Resources must be obtained where they are available" (Private sector). Similarly, "Fraud detection seems to me to be a public task par excellence. Private actors can support it (making technology available that is used by public services)" (Finances). Some suggested that the proposed data exchange platform could be developed by private actors while the standards and norms would be decided by the central administration: "interoperability standards by central administration authority. Platform (and other systems) developed by private companies (more efficient)" (Scholar). In the same vein, the use of carefully anonymized personal data as training data for private actors as a promising prospect by some participants.

However, some stakeholders did also express some mistrust towards private actors and argued in favour of a more autonomous development of IT systems and fraud fighting technologies by public actors: "No private institution aims to make the government function better. So, there is no alternative but to take matters into our own hands as a government" (Social security). A need for caution when collaborating with private actors was also voiced by many respondents. Precautions, such as the strict anonymisation of the personal data shared with private actors, are needed. It is important that the "contribution of private actors is always controlled and takes place in a strict legal-technical framework" (Federal administration).

The third main category of results concerns the many challenges faced by administrations regarding the integration of new technologies. Many stakeholders stressed a lack of internal skills and expertise as central challenge for administrations. Some specifically described a scarcity of knowledge about

"data semantics" (Federal administration) in administrations. This lack of skills and expertise was often associated with the difficulties of the public sector in achieving a reduction of its dependence towards private actors. As such, many stakeholders mentioned the need for a greater internalization of expertise to reduce dependence: "Developing certain digital skills internally will benefit independence" (Social security). Some participants also mentioned that there are important disparities between administrations regarding IT expertise which can in turn complicate data exchanges between administrations.

The lack of internal expertise was also closely linked with the lack of resources within the public sector. According to stakeholders, the lack of resources affects administrations' ability to maintain job attractiveness and internalize IT expertise: "It will not be possible to internalize this at FPS BOSA either, unless there are more flexible working conditions there (higher pay, flexible hours, fringe benefits, etc.)" (Finances). This lack of resources was also described as an obstacle to the development of new projects. For instance, some participants underlined that the creation and the monitoring of the proposed data exchange platform would require considerable resources from the public sector.

On the topic of coordination and interoperability between administrations, it seems that many challenges are rooted in the way administrations operate in the Belgian context. Among such organisational obstacles, a prominent issue voiced by stakeholders is the tendency of administrations to operate in Silos, which makes them unaware of what data is collected and stored in the databases of other administrations. Administrations are "not thinking in networks" (Regional administration), which makes it difficult to "find appropriate contacts within other government agencies that provide data" (Social security). Some stakeholders described a lack of wilfulness to share data with other administrations because the process is considered as "cumbersome and slow" (Finances) or because services try to protect their specificities. They described a general "Lack of long-term strategic vision" (Federal Administration) regarding the sharing of data between administrations. Some participants also mentioned the lack of political will as a possible detrimental factor. Such a misalignment in political and institutional priorities can further encourage divergences between administrations over time.

In addition to organisational obstacles, stakeholders mentioned the practical and technical difficulties in achieving interoperability. Data is fragmentated across administrations and, in some instances, the existing data is unstructured and unusable in its current state: "Files of judicial investigations (justice/police) are often still on paper, sometimes only partly digitized" […] it is unstructured data. Interoperability would then require that a central e-discovery platform be set up" (Finances). Stakeholders also highlighted the lack of common procedural and technical standards that would ease data exchange and interoperability across administrations from different policy sectors: "The biggest barrier to interoperability between government services is the establishment of and adherence to sufficient common technical standards for data exchange and application integration (technical interoperability)" (Regional administration).

The fourth main category of results concerns stakeholders' general reflections about the advantages and limitations of decentralized and centralized approaches. Decentralized approaches appeared as desirable for a significant number of stakeholders. These respondents argued that a decentralization of data provides greater security than centralized approaches. An excessive centralization of data was presented as a source of mistrust among citizens: "Too much centralization creates a feeling of loss of

control among citizens" (Social Security). Some also argued in favor of the BCSS model that, according to them, encompasses the advantages of a somewhat decentralized approach to data management.

Despite arguments in favour of a decentralized approach to data management and storage, many expressed some reservations. More specifically, some were unconvinced that decentralization would generate trust among citizens: "Decentralized means that data is distributed to multiple parties. This creates distrust" (Social security). Instead, a centralized but transparent approach to data management and storage would be more beneficial for citizen trust: "a centralized approach, but in full transparency and with a sound infrastructure and governance will do good for trust" (Private sector). Others viewed decentralization as too complex and abstract for citizens to be a considered as suitable solution. The relevance of a decentralized approaches was questioned by some participants who considered the use case unclear: "Use case not clear: Blockchain can be useful to make certificates unforgeable for example, but not sure of the added value on a larger scale" (Social security). A few stakeholders also signaled our lack of hindsight and questioned the technological maturity of decentralized solutions.

Some stakeholders expressed a preference for a hybrid approach with the idea that governance and management should remain centralized while storage can be decentralized. Although some degree of decentralization can be introduced, "The unique 'key' must be managed by a reliable manager" (Federal administration). Others advocated for a combination of centralized and decentralized approaches for data storage: "A centralized platform with metadata is needed. Transactional data can remain local. Master data and repositories should also be centralised" (Social Security).

The fifth main category of results concerns the role and necessity of an adequate legal framework in the process digital transition. Many stakeholders stressed the lack of a comprehensive legislation on data exchange between administrations. At the national level, stakeholders mention that the current framework imposes legal barriers that complicate data exchange and processing, especially across different policy sectors: "There is still a lack of transversality with the tax authorities (legal obstacles exist" (Social security). This issue is also present between the different government levels in Belgium. Some mentioned a "lack of alignment between laws and regulations at different levels of government" (Regional administration) as well as between European counterparts.

Many stakeholders also insisted on making sure that the proposed design solutions, such as the data exchange platform and the digital wallets, fit within a clear legal framework and that they comply with the existing legal requirements in terms of privacy protection: "Taking into account legal restrictions, it should be possible to build a central platform for data" (Private sector). Some warned that the priority should be given to adapt new IT tools to the legal framework instead of adapting the legal framework to new IT developments. Stakeholders also commented on regulatory sandbox approaches and their feasibility. Many viewed regulatory sandboxes as a viable and innovative approach to better articulate the legal framework with the adoption of new IT tools in the fight against fraud: "Especially if legislation and new technological developments are developed simultaneously and iteratively with digital legislation also following a principle of public dev (pre-release) to public prod (release)" (Federal administration). Some did however doubt the legal feasibility of regulatory sandboxes (especially with the RGPD) while others stressed the need for clear rules and guidelines surrounding the use regulatory sandboxes.

Similarly, many stakeholders insisted on the need for a clear and adequate legal framework to allow for an understandable and practical data governance. As such, some stressed the necessity to adapt and uniformise the current legal framework and guidelines to facilitate the task of privacy actors, such as DPOs: “A uniform framework would simplify this exercise and allow for a greater focus on the essence: assessing proportionality” (Finances). Other participants advocated for a re-connection between the legal framework and the current realities of IT developments: “the drafting of laws should be less disconnected from IT but also from business” (Justice). These respondents tended to positively consider “the inclusion of more IT expertise in the legislative process around digitization” (Federal Administration).

A considerable number of stakeholders also addressed the topic of explainability. Being able to explain how AI-assisted fraud decisions are reached is a necessity and it should conform to existing rules, including the GDPR: “It is a necessity, as it is both ethically and legally difficult to leave fraud fighting to an AI algorithm that cannot be explained clearly” (Federal administration). However, many participants stressed the necessity to find an equilibrium between explicability of algorithms and their effectiveness in detecting fraud. The risk is that being too transparent might help fraudsters adapt to new fraud detection techniques. Thus, some argued that the degree of transparence regarding how decisions are reached should be subjected to a risk-benefit assessment or defined legally. Still on the topic of explainability, some stakeholders insisted on the necessity to keep humans actively involved in the monitoring and follow-up of fraud detection processes that rely on AI: “it is very important to keep 'human' control after an AI analysis” (Finances). And for that purpose, it is again important to rely on a sound legal framework.

The sixth main category of results concerns stakeholders’ views on the distribution or responsibilities in digital governance. Most participants agreed that there is a need of an entity in charge of coordinating, developing, and monitoring digital projects within administrations. However, some stakeholders warned that this new entity should make sure “listen to the entities and respond to the needs of each entity (tailor-made), otherwise individual initiatives will reappear very quickly, and it will lose its strength (cf. BOSA)” (Justice). Yet, a few participants did not agree with the creation of a new entity in charge of coordinating, developing, and monitoring digital projects. They argued that, although some entity should be given this task, a completely new entity should not be created. Instead, it would be better to rely on existing structures and avoid a multiplication of actors that would complicate management: “What is needed is a simplification. The less actors there are, the less interoperability problems arise...” (Private sector).

Stakeholders also reflected on whether if the regulation of data governance should be left to public authorities or not. Most participants considered that it is indeed the role of public actors to be put in charge of the regulation of data governance: “It is the role of the public sector to assume this regulatory role” (Social security). As such, a considerable number of participants voiced their preference in favour of a federal administration for handling the coordination, development, and monitoring of future digital projects in Belgium. More specifically, most argued in favour of FPS BOSA to assume this task: “Given the data, the legal sensitivities, and perceptions, this should be given to an FPS. The mission of BOSA is clear - to serve others. This approach also allows for direct progress since the solutions exist and the legal framework does not require major adaptation” (Federal administration). Some others voiced their preference for a federal administration but without designating BOSA as the most likely candidate. An inter-federal agency, with representatives of the

different SPFs concerned, was also proposed as possible solution. A few other stakeholders argued in favor of a new entity inspired by the SMALS model (not-for-profit government organization) because of its more independent nature. Although most agreed that the regulation of data governance should be left to public authorities, some advocated that the technical aspects of the system could be developed by private actors.

Some stakeholders did however formulate some misgivings regarding the central role of the public managers in regulating data governance. Indeed, some argued that public authorities should not bear these responsibilities alone and that the private sector and/or citizens should be associated to the data regulation process: "the private sector cannot be the regulator but there must be collegiality and representativeness of user entities in the regulation (not a single manager)" (Justice). In other words, along with public authorities, citizens and companies should "have an active role in defining a governance model" (Not-for-profit organization). Some specifically argued that citizens should be associated to the process notably because it would be detrimental for trust if the responsibility "is left solely to public managers to determine the rules of data exchange" (Not-for-profit organization). A few however argued that the regulative task should not be entrusted to public authorities altogether: "this role should be fulfilled by a control body that is totally independent of the public services and political power" (Private sector).

The seventh main category of results covers stakeholders' reflections regarding the technical soundness and feasibility of some of our proposed solutions. Some stakeholders agreed with the technical feasibility of our proposed common data exchange platform. Some took other existing projects and the CBSS model as a proof that the creation of such a platform should be possible without any major obstacles. On the technical level, a considerable number of participants also mentioned the existence of systems that they already consider close, or similar, to the proposed data exchange platform. Several participants argued that such a platform system already exists, or at least partially, at the regional and federal level. They notably mentioned the existence of service integrators, which already serve the purpose of facilitating the sharing of data between administrations at the federal and the regional level: "with the MAGDA data-sharing platform, we already have a platform for data exchange that works on the basis of common criteria and technical standards" (Regional administration). Instead of a data exchange platform a suggestion was the development of a public *data lake*. However, many stakeholders stressed that the development of such a platform would stress the technical and operational capabilities of public actors. As such, many agreed that federal services would have to resort to the technical expertise and resources of the private sector. Although achieving an adequate collaboration with external partners on such a large project would prove difficult because "without knowledge of the subject matter (legislation, how something works in practice, ...)" (Finances) external contractors' contribution would not be optimal.

Some stakeholders were concerned about the technical maturity of XAI solutions, arguing that the validity of such systems was not yet demonstrated: "It has yet to be demonstrated by academic research that for certain types of AI (e.g., deep learning) it is indeed possible to design and build better traceability of their operation and their results" (Regional administration). Others noted that the fundamental flaws of AI could not be surmounted in the past few years. A few stakeholders did however mention that tests and experimentations were already ongoing for such systems, alluding to the technical validity of XAI solutions. The complexity of XAI was also a concern for some participants

who doubted that administrations would have the needed expertise to understand and use these tools.

Regarding digital wallets, several participants voiced concerns about the degree of security that such solutions would provide. They argued that the multiplication of wallets by different issuers could lead to security risks: “Citizens don't want 'wallets'... they want to be able to manage their data in a secure way” […] “The multitude of wallets could lead to security risks...” (Federal Administration).

A few stakeholders also questioned the technological maturity of decentralized solutions, arguing that we still lack hindsight on some of their aspects and implications. For instance, it was argued that some uncertainties remain regarding the soundness of the added security brought by blockchain solutions: “Decentralized data storage solutions (especially the Blockchain) raise many questions: 1) What is the added value, knowing that the encryption of data which is secure today may not be secure tomorrow because of the rise of computational capabilities. 2) Maturity of the technology: we have no hindsight” (Social security).

Finally, some other general reflections were raised on technical aspects. Some stakeholders were concerned about the general adaptability of our proposed solutions to future challenges (incl. XAI and the data exchange platform). They argued that technology evolves at such a rapid pace that new unforeseen challenges would likely arise soon. Hence, they warned that our model should probably better take into consideration this aspect. Stakeholders also reflected on the origin of the IT solutions that should be adopted. Most stakeholders voiced their preference for both national and EU IT solutions. Both options were considered adequate regarding the issue personal data protection because they should integrate national and European standards by design: “Favouring national and/or EU actors makes it easier to ensure compliance with the GDPR” (Justice). Combining both national and EU IT solutions should also allow to participate to a common (European) strategy and contribute to interoperability between the services of different EU countries while keeping in touch with local specificities. Other Stakeholders only argued in favour of European solutions considering that the GDPR legislation is an adequate groundwork on which to build new IT solutions for public services. Furthermore, they stressed that the EU has sufficient resources for the development of such tools mentioning the existence of several promising European projects, such as GAIA-X or European decentralized solutions, that should play an important role in achieving IT sovereignty in the EU. A few stakeholders did however voice a preference for national IT solutions because the adoption EU IT solutions appeared too complex and far-fetched in their opinion. On the contrary, national IT solutions seem the most realistic to these participants.

SYNTHESIS OF MODEL TESTING

We relied on eight evaluation criteria for the purpose of testing the validity of our design artefact (the proposed governance model): overall efficacy; overall suitability; feasibility; stakeholder endorsement; cognitive aspects; overall consistency; overall simplicity; and sustainability. Each of the close-ended questions used in the Delphi survey were devised to assess a key aspect of our model based on one of those criteria. This allowed us to assess participants’ level of agreement about the feasibility, overall efficacy, overall simplicity, etc. of our proposed design solutions. We applied a 65% benchmark for each criterion. In other words, we considered that our design artefact validates a given criterion if 65% of participants either agree, or partially agree in their answers to all the questions

pertaining to this criterion. Participants' level of agreement was determined using a combination of simple descriptive statistics and open-coding of participants' full set of answers across the survey questions. Main results for each criterion are as follows:

- **Overall efficacy**. This criterion assesses if the proposed governance model is perceived as an effective and efficient solution for the integration of new technologies in the fight against tax fraud and social security infringements. In total, four questions did address the efficacy of our proposed solutions: question 1.1; question 2.2; question 3.1; and question 5.1. On average, 84 % of participants either agreed, or partially agreed with the effectiveness of the design (32 % of participants agreed; 52 % of participants partially agreed; 12.8 % disagreed; 3.2 % had no opinion). This indicates that our design artifact meets the efficacy criterion.
- **Overall suitability.** This criterion assesses if the proposed governance model is perceived as a useful and relevant solution for the integration of new technologies in the fight against tax fraud and social security infringements. In total, three questions did address the suitability of our proposed solutions: question 1.2; question 1.3; and question 4.1. On average, 76.9 % of participants either agreed, or partially agreed with the suitability of the design (29.5 % of participants agreed; 47.4 % of participants partially agreed; 15.8 % disagreed; 7.3 % had no opinion). This indicates that our design artifact meets the suitability criterion.
- **Feasibility**. This criterion assesses if the design solutions of the proposed governance model can be considered feasible on a political / financial / technological / legal level. In total, four questions did specifically address the feasibility of our proposed solutions: question 2.3; question 3.3; question 5.2; question 6.3. On average, 81.3 % of participants either agreed, or partially agreed with the feasibility of the design (43.2 % of participants agreed; 38.1 % of participants partially agreed; 5.1 % disagreed; 13.6 % had no opinion). This indicates that our design artifact meets the efficacy criterion.
- **Stakeholder endorsement**. This criterion assesses if stakeholders agree with and trust the design solutions of the proposed governance model and if they are satisfied with the outcomes. No question did specifically address stakeholder endorsement in the survey. Instead, this criterion was assessed via a thematic analysis of each participant's full set of answers. Open coding was then used to assess each participant's endorsement of the model. On average, 74.3 % of participants either endorsed, or partially endorsed the design (28.6 % of participants did endorse the proposed design artefact; 45.7 % of participants did partially endorse the model; 17.1 % did not endorse it; 8.6 % had no clear position). This indicates that our design artifact meets the stakeholder endorsement criterion.
- **Cognitive aspects**. This criterion assesses if the proposed governance model promotes knowledge and information exchange among stakeholders and if it fosters cognitive learning about the policy and its implications. One question did specifically address the cognitive aspects in our design: question 4.4. On average, 78 % of participants either agreed, or partially agreed regarding the ability of the design to foster cognitive learning and knowledge exchange (57 % of participants agreed; 21 % partially agreed; 14 % disagreed; 7 % had no opinion). This indicates that our design artifact meets the cognitive criterion.
- **Overall consistency**. This criterion assesses if the proposed governance model is perceived as coherent, consistent, and sufficiently detailed. No question did specifically address the overall consistency of the design artefact in the survey. Instead, this criterion was assessed via a thematic

analysis of each participant's full set of answers. Open coding was then used to assess each participant's perception of the consistency of the model. On average, 82.8 % of participants either agreed, or partially agreed upon the overall consistency of the design (17.1 % agreed; 65.7 % partially agreed; 8.6 % disagreed; 8.6 % had no clear position). This indicates that our design artifact meets the consistency criterion.

- **Overall simplicity**. This criterion assesses if the proposed governance model is considered simple enough to be understandable and accessible by stakeholders. In total, two questions did specifically address the simplicity of our proposed solutions: question 4.3; question 6.1. On average, 69.1 % of participants either agreed, or partially agreed regarding the simplicity of the design (27.3 % of participants agreed; 41.8 % partially agreed; 12.7 % disagreed; 18.2 % had no opinion. This indicates that our design artifact meets the simplicity criterion.
- **Sustainability**. This criterion assesses if the proposed governance model is resilient to changes and unforeseen events and if it can adapt and evolve in response to future challenges. In total, three questions did specifically address the model sustainability: question 4.2; question 5.3; question 6.2. On average, 81.4 % of participants either agreed, or partially agreed regarding the sustainability of the design (42.7 % of participants agreed; 38.7 % of participants partially agreed; 6.6 % disagreed; 12 % had no opinion). This indicates that our design artifact meets the sustainability criterion.

Overall, our design artefact validates each of these criteria. This means that, to a certain degree, the proposed design artefact can be considered as an effective, suitable, feasible, consistent, simple, and sustainable governance model for the integration of new technologies in the fight against tax fraud and social security infringements. This also means that there is a reasonable endorsement of the proposed model among stakeholders and that they agree on the learning and cognitive advantages that such a model would bring for the involved parties.

That being said, some specific aspects of the model gave rise to mixed reactions among stakeholders. As such, many participants only partially agreed with the question statements presented in question 1.1 (67%) regarding the ability of the model to propose an effective response to the lack of trust among citizens. This was also observed for question 1.2 (59 %) regarding the suitability of a generalization of digital wallet systems in fostering citizen trust; question 1.3 (59 %) regarding the suitability of a decentralized approach to data management in fostering citizen trust; question 3.1 (61 %) regarding the effectiveness of the proposed model solutions in limiting the dependence of public actors; question 3.3 (50 %) regarding the feasibility of a federal service assuming the development and the technical management of a new data exchange platform; and question 5.3 (55.5 %) regarding the sustainability of fraud fighting effectiveness given the increased explicability of new fraud detection tools. Similarly, a considerable proportion of participants disagreed with the question statements presented in question 1.2 (19 %) regarding the suitability of a generalization of digital wallet systems in fostering citizen trust; question 1.3 (21 %) regarding the suitability of a decentralized approach to data management in fostering citizen trust; and question 4.3 (22%) regarding the understandability of the proposed data governance for all the actors concerned by the protection of personal data. For each of these questions, we invite to consider the results of our qualitative analysis of participants' argumentative answers. This analysis should bring useful insights as to why a considerable number of participants either partially agreed or disagreed with our suggestions on these specific topics.

GENERAL CONCLUSION OF THE DELIVERABLE

This deliverable reported on the implementation of our Delphi survey as part of the testing phase of the living-lab process. It also focused on the presentation of the results of an analysis of the collected data as well as on the evaluation of our proposed governance model for the use of new digital technologies in the fight against fraud in the social security and taxation domain.

1st objective: present an activity report for the testing phase of the living lab process. In section 2, we reported on how the survey was conducted, providing details on the methods, survey design, survey participants, and the various steps that were undergone. Then, in section 3, panelists' answers were analyzed using a combination of qualitative (thematic analysis) and quantitative methods (descriptive statistics). These results, and in particular the qualitative analysis of participant's answers, provides us with a crucial input as it will help us refine the next iteration of our design artefact and contribute to the construction of a proof-of-concept governance model.

2nd objective: report on the results of our analysis of the collected data. In section 3, we reported the main results of a combination descriptive statistics and a qualitative analysis of participants' answers to the survey. The main findings were further discussed in section 5. Main findings can be summarized as follows : 1) Technical solutions alone (e.g., digital wallet solutions, decentralized approaches) would not support citizen trust; 2. The collaboration with private actors appears as a much-needed compromise; 3. Working in networks might foster interoperability and mitigate resource limitations; 4. There is no clear consensus among stakeholders regarding the choice between centralized and decentralized approaches (or a mix of both); 5. Relying on a "regulatory sandbox" approach might help in producing a clear, transparent, and adaptive legal framework; 6. The central role of federal authorities in data governance and the need to associate civil society representatives to governance choices.

3rd objective: test the validity of our design artefact presented in D3.3. (a governance model for the use of new digital technologies in the fight against fraud in the social security and taxation domain). The qualitative and quantitative analysis were also instrumental in testing the validity of our proposed governance model. Indeed, the fourth section of this deliverable focused on the assessment of our model based on eight evaluation criteria: overall efficacy; overall suitability; feasibility; stakeholder endorsement; cognitive aspects; overall consistency; overall simplicity; and sustainability. These criteria were selected based on a literature review on the criteria that are commonly used for testing in design science research as well as in the planning and public policy evaluation literatures. After applying a 65% benchmark for each criterion (a criterion is respected if 65% of participants either agree, or partially agree in their answers to all the questions pertaining to a given evaluation criterion), we conclude that our proposed governance model respects all the criteria that were selected to assess its validity.

Although benchmarks were respected for all the selected criteria, many aspects of the model still resulted in mixed reactions among the stakeholders who participated in the survey. For instance, a large proportion of participants indicated that they only partially agreed with the question statements presented in question 1.1; question 1.2; question 1.3; question 3.1; question 3.3; and question 5.3. Similarly, a sizeable proportion of participants disagreed with the question statements presented in question 1.2; question 1.3; and question 4.3. Hence, we strongly suggest that any further adaptations

to our model should take into consideration the results of the qualitative analysis of participants' answers to these specific questions.

We finally conclude the present deliverable by acknowledging a few limitations pertaining to the Delphi method that we used in this research.

- The first limitation concerns the possible risk of researcher bias when conducing a Delphi survey. Indeed, when "performing a Delphi, the researcher is in a powerful and influential position and as such, knowingly, or unknowingly can significantly bias the study" (Vernon, 2008, p. 74). Among such potential bias, are the choice, formulation, and presentation of the survey questions (Linstone & Turoff, 1975; Vernon, 2008; Franklin & Hart, 2007). Building a Delphi survey questionnaires is a notoriously challenging endeavor (e.g., Franklin & Hart, 2007) and this was no exception in our study. To minimize the risk of bias, we submitted draft versions of our survey to several colleagues throughout the questionnaire building process. We made sure to address their concerns regarding the choice and formulation of our survey questions.
- Another possible researcher bias can be exerted during the construction of the panel of experts (Linstone & Turoff, 1975; Vernon, 2008; Franklin & Hart, 2007). Indeed, there can be a "temptation for a researcher to select panel members with known positions on the problem" (Avella, 2016, p. 315). Although we tried to remain objective and unbiased when mapping the ecosystem of actors that we ultimately included in the panel of experts for the present survey, it is possible that we overlooked some actors due to the multiplicity of the involved parties. To address this potential issue, we also invited stakeholders to share with us the references of any additional expert that might be interested in participating in our survey.
- Finally, several complementary rounds of the Delphi survey could have been organized in order to gain additional insights on how to further refine our governance model. Although the current survey results are already particularly insightful for our design research purposes, higher levels of consensus among stakeholders regarding some of specific design solutions might have been achieved with the help of additional survey rounds. However, additional survey rounds would have been challenging to implement due to practical limitations and time constraints (given the research project timeframe). This observation stresses the demanding characteristic of Delphi surveys, which often require considerable time and investment from researchers.

6. REFERENCES

Avella, J. R. (2016). Delphi panels: Research design, procedures, advantages, and challenges. *International Journal of Doctoral Studies, 11*, 305.

Brady, S. R. (2015). Utilizing and adapting the Delphi method for use in qualitative research. International Journal of Qualitative Methods, 14(5), 1609406915621381.

Delbecq, A. L., Van de Ven, A. H., & Gustafson, D. H. (1975). Group techniques for program planning: A guide to nominal group and Delphi processes. Scott, Foresman.

Fallon, C. (2018). Interpretative analysis of decentralized policy with the use of an online Delphi, ECPR General Conference, Hambourg, 25/8/2018.

Franklin, K. K., & Hart, J. K. (2007). Idea generation and exploration: Benefits and limitations of the policy Delphi research method. *Innovative Higher Education, 31*(4), 237-246.

Hasson, F., Keeney, S., & McKenna, H. (2000). Research guidelines for the Delphi survey technique. Journal of advanced nursing, 32(4), 1008-1015.

Landeta, J. (2006). Current validity of the Delphi method in social sciences. *Technological forecasting and social change*, *73*(5), 467-482.

Linstone H.A. & Turoff M. (1975) The Delphi Method. Techniques and Applications. Addison-Wesley, Reading, Massachusetts.

Miles, M., & Huberman, A. M. (1994). Qualitative data analysis: An expanded sourcebook. Thousand Oaks, CA: Sage.

Paillé, P., & Mucchielli, A. (2021). *L'analyse qualitative en sciences humaines et sociales-5e éd*. Armand Colin.

Plesch, C., Kaendler, C., Rummel, N., Wiedmann, M., & Spada, H. (2013). Identifying areas of tension in the field of technology-enhanced learning: results of an international delphi study. *Computers & Education*, *65*, 92-105.

Schneider, J. B. (1971). The policy Delphi: A regional planning application. Technological Forecasting and Social Change, 3, 481-497.

Shariff, N. (2015). Utilizing the Delphi survey approach: A review. *J Nurs Care*, *4*(3), 246.

Sharkey, S. B., & Sharples, A. Y. (2001). An approach to consensus building using the Delphi technique: developing a learning resource in mental health. Nurse education today, 21(5), 398-408.

Sharma, R. S., & Yang, Y. (2015). A hybrid scenario planning methodology for interactive digital media. *Long Range Planning*, *48*(6), 412-429.

Skulmoski, G. J., Hartman, F. T., & Krahn, J. (2007). The Delphi method for graduate research. Journal of Information Technology Education: Research, 6(1), 1-21.

Strauss, A., & Corbin, J. (1998). *Basics of qualitative research techniques* (pp. 1-312). Thousand oaks, CA: Sage publications.

Van Dijk, J. A. (1990). Delphi method as a learning instrument: bank employees discussing an automation project. *Technological Forecasting and Social Change*, *37*(4), 399-407.

Vernon, W. (2009). The Delphi technique: a review. *International Journal of Therapy and rehabilitation*, *16*(2), 69-76.