

Dipartimento di Informatica, Bioingegneria,
Robotica ed Ingegneria dei Sistemi

**An Assisted Methodology to Conduct Data
Protection Impact Assessment**

by

Salimeh Dashti

Theses Series

DIBRIS-TH-2021-XX

DIBRIS, Università di Genova

Via Opera Pia, 13 16145 Genova, Italy

<http://www.dibris.unige.it/>

Università degli Studi di Genova

Dipartimento di Informatica, Bioingegneria,

Robotica ed Ingegneria dei Sistemi

Ph.D. Thesis in Computer Science and Systems

Engineering

Computer Science Curriculum

**An Assisted Methodology to Conduct Data
Protection Impact Assessment**

by

Salimeh Dashti

July, 2021

**Dottorato di Ricerca in Informatica ed Ingegneria dei Sistemi
Indirizzo Informatica
Dipartimento di Informatica, Bioingegneria, Robotica ed Ingegneria dei
Sistemi
Università degli Studi di Genova**

DIBRIS, Univ. di Genova
Via Opera Pia, 13
I-16145 Genova, Italy
<http://www.dibris.unige.it/>

**Ph.D. Thesis in Computer Science and Systems Engineering
Computer Science Curriculum
(S.S.D. INF/01)**

Submitted by Salimeh Dashti
DIBRIS, Univ. di Genova and Security & Trust Research Unit, Fondazione Bruno
Kessler, Trento, Italy
sdashti@fbk.eu

Date of submission: May 2021

Title: An Assisted Methodology to Conduct a Data Protection Impact Assessment

Advisor: Silvio Ranise
Professor, Department of Mathematics, University of Trento, Trento, Italy & Head
of Impact Area Cybersecurity, Fondazione Bruno Kessler, Trento, Italy

Ext. Reviewers:

Luca Viganò Professor, Head of Cybersecurity Group, King's College London,
England, United Kingdom luca.vigano@kcl.ac.uk

Erisa Karafili Assistant Professor, University of Southampton, England, United
Kingdom e.karafili@soton.ac.uk

Abstract

The uptake of digital technologies in our everyday activities today is unlike any time in history. Consequently, the amount of personal data produced and shared is staggering. Indeed, they have become the primary asset for many businesses. While users benefit from online engagement, an increasing number of critics have voiced their privacy concerns. To protect peoples' fundamental rights concerning processing their personal data, General Data Protection Regulation (GDPR) has been introduced. GDPR requires to conduct a Data Protection Impact Assessment (DPIA) when data processing is likely to result in a high risk to the rights and freedoms of individuals. For example, where the processing may lead to discrimination, damage to the reputation, loss of confidentiality personal data. Therefore, it requires assessing security risks and privacy risks—we learned identifying the latter is not easy even for information security and data protection experts. GDPR is not clear about when and how to conduct a DPIA. Thus, academic works and legal bodies introduced guidelines and tools to help controllers conduct the DPIA. However, these works lack to either provide an assistance, include all steps of the DPIA or be applicable to all domains. These shortages motivated us to propose an assisted methodology to conduct a DPIA. The methodology provides assistance from identifying the required data type for a given data processing to identifying and evaluating privacy and security risks.

We have adopted our methodology to conduct a DPIA-compliance risk analysis for OAuth/OIDC-based financial services. That is because of: (1) the growth of open banking, (2) the necessity of deploying appropriate identity management solutions—as stated in PSD2, which requires to respect the GDPR requirement—and (3) the wide usage of OAuth/OIDC identity management solutions that are secure but error-prone. The methodology can also be used for any OAuth/OIDC-based services.

To my parents and my little brother.
Love.

Table of Contents

List of Figures	6
List of Tables	8
Chapter 1 Introduction	10
1.1 Context and Motivation	10
1.2 Contribution	15
1.3 Structure of the Thesis	16
1.4 Publications	17
Chapter 2 Problem Definition and Reference Model	18
2.1 Problem Definition	18
2.2 Information System Reference Model	19
2.2.1 Security Reference Model	20
2.2.2 Privacy Reference Model	24
2.3 Formalization of Identified Problems	28
2.3.1 Problem P_{risk} definition	30
2.3.2 Problem $P_{compliance}$ Definition	31
Chapter 3 Can Data Subject Perception of Privacy Risks Be Useful in a DPIA?	32
3.1 Background: Quantitative Analysis	33

3.2	Motivation and Methodology	34
3.3	Results	38
3.3.1	Results of Guided Survey	38
3.3.2	Results of Unguided Survey	40
3.4	Discussion	41
3.4.1	RQ1: People’s Perception	41
3.4.2	RQ2: Experts’ Perception of Privacy Risks	43
3.5	Related Work	43
3.6	Conclusion	46
Chapter 4	Background	47
4.1	General Data Protection Regulation	47
4.2	Data Protection Impact Assessment	49
4.3	Privacy Goals	51
4.4	Privacy Strategies	52
4.5	RiskML Tool	53
4.6	Automated Access Control Compliance Checking	55
Chapter 5	An assisted Methodology to Conduct a DPIA	59
5.1	An Overview of the Methodology	60
5.2	Step 1. Processing Analysis	64
5.2.1	Overview of the Step	64
5.2.2	Introducing the Organization	64
5.2.3	Introducing Data Processing	69
5.3	Step 2. Risk Analysis	76
5.3.1	Overview of the Step	76
5.3.2	Supporting Data Subject’s Right to Data Protection	78
5.3.3	Supporting Data Subject’s Right to Privacy	82

5.3.4 Investigate vulnerabilities	91
5.3.5 Compliance of Access Control Policies	93
5.3.6 Modeling Risk	94
5.4 Related Work	101
5.4.1 Privacy risk Managements Approaches	101
5.4.2 Data Protection Impact Assessment	105
5.5 Conclusion	109
Chapter 6 Application Of Methodology On OAuth/OIDC-based Services	111
6.1 Background	113
6.1.1 Access Delegation: OAuth Standard	113
6.1.2 Single Sign On: OpenID Connect Standard	113
6.2 Problem Definition and OAuth/OIDC Reference Model	115
6.2.1 OAuth/OIDC Reference Model	116
6.2.2 Best Current Practice Specification	119
6.2.3 Problem Definition	126
6.3 Application of Our Methodology on OAuth/OIDC-based Solutions	129
6.3.1 Processing Analysis	129
6.3.2 Risk Analysis	130
6.4 Related Work	143
6.5 Conclusion	145
Chapter 7 Conclusion	147
7.1 Future Work	149
Bibliography	151
Appendix A Surveys	170
A.1 The common Parts of the surveys	170

A.1.1 The First Page	170
A.1.2 The Third Page	171
A.1.3 The Ninth Page	172
A.2 Guided Survey: Page 4 to 8	172
A.3 Unguided Survey: Page 4	174
Appendix B NIST Catalog of Problematic Data Actions and Problems	176
B.1 Problematic Data Actions	176
B.2 Problems	178
B.3 Related Privacy Enhanced Technologies to Privacy Goals	178
Appendix C The Questionnaires	182
C.1 Control Questionnaire	182
C.2 Right Questionnaire	191
Appendix D OAuth/OIDC Related Materials	200
D.1 OAuth/OIDC Features Description	200
D.2 OAuth/OIDC Complete Reference Model	200
D.3 Complete List of assessed IdMPs	200
D.4 IdMP_Doc Questionnaire	201
D.5 IdMP_ToAsk Questionnaire	203

List of Figures

1.1 A Screenshot of ICO PIA Template.	13
1.2 A Screenshot of CNIL PIA Tool.	14
3.1 The Identified Privacy risks With the Frequency of Given Impacts.	40
4.1 The DPIA Process, Proposed by [Arta].	51
4.2 An Example of RiskML Model.	56
4.3 An Excerpt of Formalization of GDPR.	58
5.1 An overview of our methodology.	60
5.2 Detailed Overview of Steps of the Methodology.	63
5.3 Annotated Message Sequence Chart of the Running Example.	75
5.4 An Excerpt of Control Questionnaire Output in JSON Format.	80
5.5 An Excerpt of Right Questionnaire Output in JSON Format.	88
5.6 Annotated Security/Privacy Risk Summary Document to Extract RiskML Model.	96
5.7 Annotated Captured Vulnerabilities Document	97
5.8 An example of Customized XML File.	97
5.9 Security Risk Model of the Running Example.	99
5.10 Privacy Risk Model of the Running Example.	100
6.1 OIDC Authorization Code Flow with Code Challenge.	114

6.2 BCPs-Compliant Request Schema	125
6.3 Static XML Model, Related to Feature Code Challenge Method	138
6.4 IBM Risk Model.	140

List of Tables

2.1	The Security Reference Model.	21
2.2	Mapping of Recital 75 Privacy Risks to Problematic Data Actions.	26
2.3	Mapping of Problematic Data Actions to Privacy Goals.	28
2.4	Privacy Reference Model.	29
3.1	Guided Survey Result.	39
3.2	Age Range Impact Analysis for Privacy Risks that Accept the H_0	39
3.3	Impact Estimations of Same Privacy Risks By Different Works.	42
4.1	Eights Privacy Strategies and their Tactics.	53
5.1	Data Type and Data Subject category related to Economic Sector	66
5.2	Related Data Processing Stage of each privacy threat.	74
5.3	Mapping Privacy Goals to Privacy Enhanced Technology	84
6.1	OIDC query parameters of Authorization Code Flow With Code Challenge.	115
6.2	OAuth/OIDC Reference Model	117
6.3	Composed Features.	118
6.4	Security BCPs for FAPI and OAuth/OIDC Security.	121
6.5	Privacy BCPs.	124
6.6	An excerpt list of known IdMPs and their supported features.	132
6.7	The Relation between IdMP features and Discovery Endpoint JSON Keys.	133

D.1 Atomic Features Description.	201
D.2 OAuth/OIDC Full Reference Model.	202
D.3 list of known IdMPs and their supported features.	205

Chapter 1

Introduction

1.1 Context and Motivation

Technology has become an indispensable part of our lives—from the moment we wake up to the moment we go to sleep and even while we are sleeping. Digital 2020¹ reported more than 4.5 billion people use the internet, while social media users have passed the 3.8 billion mark; that is, nearly 60 percent of the world’s population is already online. People engage in online activities to gain psychological [TM12], emotional [KKVG11], economical or social benefits. As a result, the amount of data we produce about ourselves and share is staggering—that offers vast business opportunities and has substantial economic value. Indeed, data have become the primary asset for many businesses. Consequently, businesses start to collect data from various sources, including business transactions, IoT devices, industrial equipment, videos, social media, etc. Every area in every business—from supply chain efficiency to overall technology innovation—can be improved through smart use of data and analytics.²

While users benefit from online engagement, an increasing number of critics have voiced their concerns over the privacy [KK12] and how data handling often entails a privacy reduction [GRV19, BMA94] by commercial exploitation of their personal data [ATW16]. Therefore, the same practice that provides values to people and organizations also raises privacy concerns [BMA94]. Yet, exploiting the commercial value of data can often entail a reduction in private utility and sometimes in social welfare overall [ATW16]. Indeed, the problem is not the data, it is who gets to see and use

¹<https://wearesocial.com/blog/2020/01/digital-2020-3-8-billion-people-use-social-media>

²<https://www.pwccn.com/en/issues/data-and-analytics/improve-business-performance.html>

those data [RD16]. The Special Eurobarometer general surveys in 2015³ [Spe15] reported that 71% out of 27,980 European people believe that providing personal information is an increasing part of modern life, while 89% overwhelmingly believe they should always have the same rights and protections over their personal data as the public authority or private company offering the service.

To protect peoples' fundamental rights concerning processing their personal information and on the free movement of such data between the Member States, the European Parliament and the council have introduced the General Data Protection Regulation (GDPR). The Regulation became enforceable beginning 25 May 2018. The GDPR aims to harmonize the protection of fundamental rights and freedoms of data subjects with respect to processing activities (recital 3). In this thesis, whenever we refer to an article or recital, we are referring to the ones stated in the GDPR.

Recital 84 says "in order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of data subjects, the controller should be responsible for the carrying-out of a Data Protection Impact Assessment (DPIA) to evaluate, in particular, the origin, nature, particularity, and severity of that risk [...]". A controller is a responsible entity to determine the purposes and means of the processing of personal data. Introduction of DPIA by the Regulation is a newcomer in the impact assessment vocabulary; on the one hand, it has no direct previous historical lineage and in this sense refers to aspects that are specific to the European Union context; on the other hand, it could be argued that it shares many similarities with the field of Privacy Impact Assessment (PIA) [VDGR16]. PIA has gradually developed, from the 1990s onward, to assess the impacts on the privacy of a project which involves the processing of personal information [WdH12]. It is a methodology to assess the impacts on the privacy of a service, which involves the processing of personal data for taking action to prevent or minimize negative impacts [WdH12]. PIA has been widely adopted and studied, (see e.g., [Artb, Artc, VDGR16, Cla09, Wri12, OS14, Cla99, Spi12, CK13, ICO14, CNI15]) and has been published for a number of specific products [Spi12, CK13], and used in different countries, such as: Australia, Canada, Ireland, New Zealand, the United Kingdom, and the United States. However, the PIA has not been an obligation until the GDPR came to enforcement. The introduction of DPIA in the Regulation can be seen as part of a broader risk-based turn in the field of data protection regulation and legislation [VZ16].

The GDPR articulates DPIA in article 35, stating that "Where a type of processing [...] is likely to result in a high risk to the rights and freedoms of data subjects, the con-

³The Special Eurobarometer general surveys in 2015 explores how people feel over the personal data they provide online.

troller shall, before the processing, assess the impact of the envisaged processing operations on the protection of personal data”.

When should a DPIA be conducted? The DPIA shall be conducted when data processing is likely to result in *high risks to the rights and freedoms of data subjects*. Recitals 89 and 91 along with article 35 provide a list of processing operations that are by default considered likely to present high risks to rights and freedoms of data subjects, e.g., when data processing involves: new technologies, large scale of special category of data, and systematic monitoring of a publicly accessible area on a large scale—the lists is indicative/non-exhaustive [Dem19]. There is no further elaboration; it is not even clear what large scale means. The Guidelines on Data Protection Officers (WP243) [Boa] provides some example of large-scale that includes: processing of the patients data by a hospital, processing of individuals’ travel data using a city’s public transport system, processing of data by an insurance company or a bank. Yet, the definition of large scale is scarce.⁴ The EDPB⁵ states that where it is not clear whether a DPIA is required, a DPIA is carried out nonetheless [Arta]. The office of the Australian Information Commissioner stated that the first question to ask about whether a DPIA is needed is “will any personal information be collected, stored, used or disclosed in the project?” If the answer is yes, then a DPIA is probably necessary [oAIC14]. Authors in [VvdB17] also argue that it would be the case for most of data processing to require the DPIA, as data processing puts the fundamental rights of data subjects at risk. Moreover, a risk assessment shall be conducted, anyways. As the GDPR asks to identify and evaluate the risks to rights and freedoms of data subjects, and introduce proper countermeasures in different articles, such as articles 24, 25 and 35. To this end, controllers need to conduct a DPIA, unless they can demonstrate that there is not likely that their processing lead to high risks to data subjects’ rights and freedoms—which one can know only when s/he conduct a DPIA, as recital 84 states.

How should a DPIA be conducted? Article 35.7 provides a minimum guideline for carrying out the DPIA, and does not lay down any further details—it is unclear how to conduct a DPIA, as argued also in [AS17, CFKA18, VDGR16, DLM16, BFH⁺16, VK18]. Therefore, different legal bodies and academics (see e.g., [CNI18, ICO18, Arta, BFH⁺16, CFKA18, ASRJ18, SWBS19, ACDC⁺15]) started to introduce guidelines and tools to help controllers conduct the DPIA. These works are short in either providing assistance (they work more like a checklist), including all steps of the DPIA (e.g., monitoring), or being applicable to all domains. Among others, the Informa-

⁴<https://iapp.org/news/a/on-large-scale-data-processing-and-gdpr-compliance/>

⁵The Article 29 Working Party is the independent European working party that dealt with issues relating to the protection of privacy and personal data until 25 May 2018—entry into application of the GDPR. Since it has been replaced by the European Data Protection Board (EDPB).

tion Commissioner’s Office (ICO)⁶ and the Commission nationale de l’informatique et des libertés (CNIL)⁷ have proposed tool to conduct DPIA. Figure 1.1 and 1.2 show screenshots from ICO DPIA Template [ICO] and CNIL PIA tool [CNI], respectively. As can be seen, they ask controller fill a form(s)—no assistance is provided at any step of the process, they are checklists. While, the controller needs to have a more elaborated guidance/tool to objectively assess the risks [Dem19] and carry a DPIA.

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals’ views – or justify why it’s not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm	Severity of harm	Overall risk
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

DPIA template
20180622
v0.4

5

DPIA template
20180622
v0.4

6

Figure 1.1: A Screenshot of ICO PIA Template.

What does DPIA require? The DPIA requires to protect data subjects against the risks to their rights and freedoms; that is a new perspective to risk. Recital 75 lists some example of such risks: where the processing gives rise to discrimination, social disadvantage or damage to reputation. Risk to rights and freedoms is an abstract

⁶The Information Commissioner’s Office (ICO) is an independent regulatory office dealing with the Data Protection Act 2018 and the General Data Protection Regulation, the Privacy and Electronic Communications (EC Directive) Regulations 2003 across the n England, Wales and Northern Ireland and, to a limited extent, in Scotland. It reports directly to the Parliament of the United Kingdom.

⁷The Commission nationale de l’informatique et des libertés (CNIL) is an independent French administrative regulatory body whose mission is to ensure that data privacy law is applied to the collection, storage, and use of personal data.

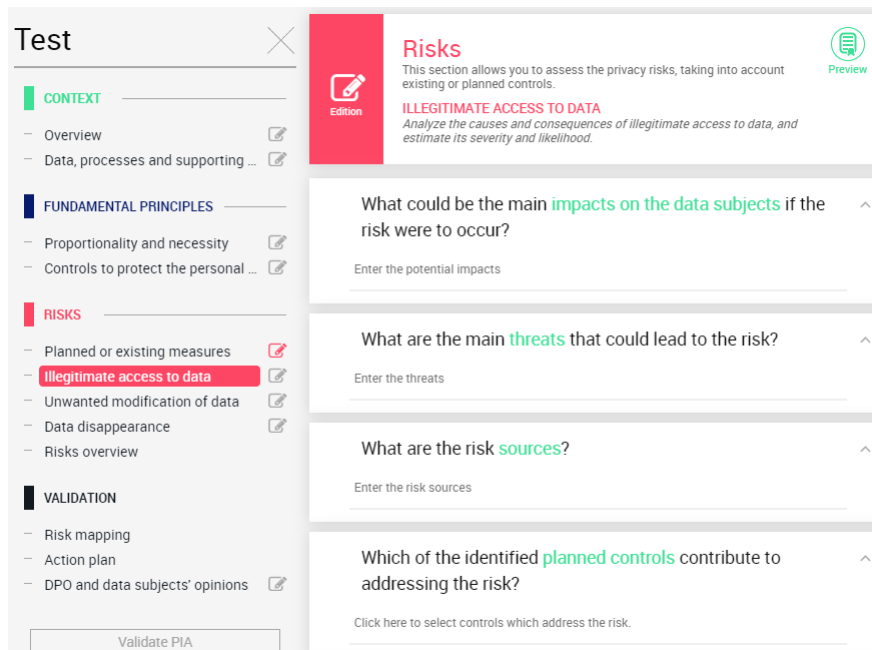


Figure 1.2: A Screenshot of CNIL PIA Tool.

and subjective concept. Surveying 84 information security and privacy experts, we learned that even experts confuse privacy risks with security risks (See Chapter 3). One of the data subjects' rights is the right to data protection (recital 78). Controllers require to take into account the technical and organizational measures for ensuring the security of the processing (article 32). Therefore, controllers not only need to identify privacy risks, but also to identify security risks to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

The aforementioned requirements challenge controllers to conduct a DPIA. That motivated us to ensure that controllers get assisted in conducting a DPIA to ensure compliance. We propose an iterative assisted methodology to conduct a DPIA that comprises three steps: *Processing Analysis*, *Risk Analysis* and *Run-time Analysis*. The first step is to determine the context of analysis by identifying the roles, purpose, involved data type and data subjects, etc. The second step is to capture both privacy and security risks that data processing might pose, and model and evaluate them. The last step is to monitor the system to ensure its compliance throughout the data processing lifecycle. In each step, we assist controllers. For example, to identify privacy risks—that are uneasy to identify—we list bad actions which may lead to privacy risks. We map the bad actions to their related privacy risk (see Section 5.2.3). The actions are concrete and easy to identify.

An application of our methodology. Open Banking emerged from the EU PSD2 regulation, whose original intent was to increase competition and innovation into the financial services sector. Although this drastic reduction of data barriers within the banking industry has led to significant product and service innovations, it comes together with risks such as loss or theft of personal data, data protection violations, etc. One of the key points to make these services trustworthy—as required by PSD2—is to deploy an appropriate identity management solution. PSD2 requires to meet GDPR requirements when personal data is processed—as in the authorization and authentication process. The controller requires to conduct a risk analysis to evaluate the likelihood and severity of risks to rights and freedoms of data subjects where processing involves a large amount of personal data and affects a large number of data subjects (recital 75). That is the case for authentication and authorization process. Among other identity management solutions, OAuth 2.0 (OAuth) and OpenID Connect (OIDC) are the two widely used ones [Sim, LM20]. They provide a secure solution, but their implementation is error-prone. Therefore, to assist controllers we have adopted our assisted methodology to conduct a DPIA-compliant risk assessment for OAuth/OIDC based solutions. Our methodology is designed to address the requirements of OAuth/OIDC-based financial services and any OAuth/OIDC-based services that process either a special category of personal data or common personal data.

1.2 Contribution

Below, we list the main contributions of this thesis work:

- Providing automated assistance for controllers to meet the security and privacy requirements of the information system in question to comply with the DPIA (Chapter 5), by:
 - building a *security* and *privacy* reference model (Chapter 2) to assess the security and privacy level and guide controllers to guarantee a minimum level—knowing the appropriate security level is not trivial [NIS13]—according to requirements of the system;
 - assisting controllers to identify privacy risks to data subjects’ rights and freedoms (Section 5.2.3)—conducting a survey, we learned that even for information security and data protection experts identifying privacy risks and differentiating them from security risks are not easy (Chapter 3);
 - assisting controllers to identify security risks (Section 5.3)—to protect

- data subjects' right to data protection, that is, to ensure appropriate security of the personal data.
- assisting controllers to identify data type and data subject categories according to the economic sector to which they belong—our experience to carry DPIA for the public administration in Trento, Italy, taught us that controllers have difficulties in identifying required categories of data and data subjects for their data processing (Section 5.2.2);
- extending RiskML tool (i.e., a tool-supported framework for risk modeling and evaluation) to automatically model the risks and providing what-if analysis for controllers to make an informed decision on configuration of the system in question (Section 5.3.6).
- Applying the methodology to conduct an assisted DPIA-compliance risk analysis for OAuth/OIDC-based online services (Chapter 6), by:
 - building an OAuth/OIDC reference model to assess the level of security and privacy of the solution;
 - checking whether the solution meet the privacy and security required by the relevant best current practice;
 - modeling and evaluating the privacy and security risks, and providing what-if analysis to assist the controller taking an informed decision on choosing the right identity provider (which meet the security and privacy requirements of the system) and the implementation of the solution.

1.3 Structure of the Thesis

The thesis is structured as follows:

Chapter 2 motivates the work and defines two problems that our proposed methodology will solve. Chapter 3 presents two conducted surveys—one to assess data subjects' perception of privacy risks, and the other to examine whether information security and data privacy experts can identify privacy risks—and their statistical analysis of their results. Chapter 4 - presents some basic concepts which are instrumental to the definition of the proposed methodology.

1. GDPR concepts Definitions—elaborates on related Regulation requirements and glossary;
2. Data Protection Impact Assessment—elaborates on requirements of the assessment, which is the main focus of this thesis work;

3. Privacy and Security Goals—explains the goals that to be fulfilled by an information system to meet DPIA requirements;
4. Privacy Strategies—elaborates on the strategies to meet the abstract notion of privacy risks;
5. RiskML tool—the adopted tool to automatically generate the risk model and importantly provide the possibility of performing what-if analysis;
6. Automated legal compliance checking tool—the adopted tool to check whether the user-specified access control policies complies with the requirements of the GDPR.

Chapter 5 presents our proposed assisted methodology to address the two identified problems. Chapter 6 presents the application of our proposed methodology on OAuth and OpenID connect-based online services. Chapter 7 concludes the thesis. Chapter 3, 5 and 6 contains related works associated to their context.

1.4 Publications

1. Salimeh Dashti, Amir Sharif, Roberto Carbone, and Silvio Ranise. Automated risk assessment and trade-off analysis of Openid connect and OAuth 2.0 deployments. In Conference on data and applications security and privacy-DBSec, 2021.
2. Salimeh Dashti, Anderson Santana De Oliveria, Caelin Kaplan, Manuel Dalcagnè, and Silvio Ranise. Can data subject perception of privacy risks be useful in a data protection impact assessment? In 18th International Conference on Security and Cryptography-SECRYPT, 2021.
3. Salimeh Dashti and Silvio Ranise. "A Tool-assisted Methodology for the Data Protection Impact Assessment." In 16th International Joint Conference on e-Business and Telecommunications (ICETE (2))-SECRYPT. Vol. 2, pages 276-283, 2019.
4. Salimeh Dashti and Silvio Ranise. "Tool-Assisted Risk Analysis for Data Protection Impact Assessment.", Privacy and Identity Management, page.308, 2020.

Chapter 2

Problem Definition and Reference Model

2.1 Problem Definition

The GDPR states that the *risks to the rights and freedoms of natural persons*, of varying likelihood and severity, may result from personal data processing, which could lead to physical, material or non-material damage, such as discrimination, identity theft or fraud, financial loss, damage to the reputation, etc. Article 35 states that “where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.”

The GDPR is not specific about when the risk is high or how to conduct a DPIA (as stated also in [AS17, CFKA18, VDGR16, DLM16, BFH⁺16, VK18]). Article 29 Working Party (replaced by EDPB) [Arta] states that where it is not clear whether a DPIA is required, a *DPIA is carried out nonetheless* as a DPIA is a useful tool to help controllers comply with data protection law. Authors in [oAIC14, VvdB17] also state that for most of data processing, it is necessary to conduct a DPIA. Several articles of the GDPR require to evaluate risk to rights and freedoms of data subjects (see e.g., article 24). Until the controller does not conduct a risk assessment, s/he cannot know if the risk is high (recital 84).

The DPIA protects data subjects’ rights. Articles 15 to 21 articulate data subjects’ rights, such as the right to access, restrict data processing, and objects. Recital

78, articles 24 and 32 require to respect their *rights to data protection*, and to implement appropriate technical and organisational measures to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services and compliance with the Regulation. Therefore, controllers not only need to consider *security risks*, but also *privacy risks* that might infringe their rights and freedoms—which are *uneasy to identify even for information security and data protection experts* (See Chapter 3)—they need hints and suggestions as recommended in [CG⁺16].

Article 5 sets out data processing principles that are a fundamental building block for good data protection practice and key to compliance with the GDPR.¹ According to article 83.5.a and b, infringements of *data processing principles and data subjects' rights* are subject to administrative fines up to 20,000,000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

To this end, controllers need to conduct a DPIA to (i) assess security and privacy risks, (ii) respect data processing principles and (iii) data subjects' rights to comply with the Regulation requirements. Meeting the above-mentioned requirements is a daunting task. Therefore, we propose an assisted methodology to perform a DPIA, in which we have considered the above-mentioned requirements. As such, we identify the following two problems:

P_{risk} security and privacy risk assessment and trade-off analysis, taking into account the risk propagation;

$P_{compliance}$ compliance assessment w.r.t. security and privacy requirements of DPIA.

Before elaborating on the problems, we introduce two reference models: security reference model (Section 2.2.1) and privacy reference model (See Section 2.2.2). Then, we formalize the two above-mentioned problems (see Section 2.3). Chapter 5 details our methodology to address the identified problems.

2.2 Information System Reference Model

We have built two reference models: *security reference model* and *privacy reference model*. The reference models guide controllers to guarantee a minimum level of

¹<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/>

security and privacy based on the impact that the data processing s/he conduct could have on the rights and freedoms of data subjects.

To build the *security reference model*, we extracted technical security controls listed in [NIS13] and categorized them based on the security goal that they address. To build the *privacy reference model* we have extracted privacy tactics introduced in [Hoe18] to address privacy goals (introduced in Section 4.3). Each extracted security control/privacy tactic protects the information system to satisfy a security/privacy goal(s). We refer to them as *Atomic Features* (*af*). We group the *af*s which aim to protect a common security/privacy goal, and call them *Composed Features* (*cf*).

Table 2.1 and Table 2.4 represent *security reference model* and *privacy reference model*, respectively. The third column of Table 2.1 lists the *af*s; and its first column reports *cfs*. For example, *af* Identification and Authentication protects security goal *confidentiality*. While, the second column of Table 2.4 reports the formula composed of *af*s, which we refer to as $DPIA_{privacy}$, and the third column of 2.4 represents the *cfs*. For example, following *af*s together allow to meet privacy goal *transparency*: *supply*, *notify*, and *explain*.

An *af* could contribute to meet more than one security/privacy goal, we call them *consecutive Goal*. The fourth column of Table 2.1 and Table 2.4 list these goals. Take again *af* Identification and authentication. Beside *confidentiality*, it contributes to protect security goal *integrity*, and not implementing it may also lead to *compromising integrity*.

Note that the controller can update the reference models and use any models that fit their information system's requirements in question. This is what we have done when applying the methodology on OAuth/OIDC-based services, that will be discussed in Chapter 6.

2.2.1 Security Reference Model

Article 32.1.b states that “taking into account state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.”

However, knowing the appropriate security level is not trivial [NIS13]. To assist organizations in making the appropriate selection of security controls for information systems to guarantee minimum security, NIST 800-53-r4 [NIS13] introduces

Table 2.1: The Security Reference Model.

Composed Feature (Sec. Goal)	Ctrl#	Atomic Feature (Security Control)	Consecutive goal	Baseline		
				Low	Moderate	High
Confidentiality	Identification and authentication (IA)					
	IA-2	Identification and authentication	Integrity	IA-2	IA-2 (3) AND (8)	IA-2 (3) AND (4) AND (8)
	IA-3	Device identification and authentication		-	IA-3	IA-3
	IA-4	Identifier management		IA-4	IA-4	IA-4
	IA-5	Authenticator management		IA-5	IA-5 (2) AND (3)	IA-5 (2) AND (3)
	IA-7	Cryptographic module authentication		IA-7	IA-7	IA-7
	IA-8	Identification and authentication (non-organizational users)		IA-8 (2) AND (3) AND (4)	IA-8 (2) AND (3) AND (4)	IA-8 (2) AND (3) AND (4)
	Access control (AC)					
	AC-2	Account management	Integrity	AC-2	AC-2 (3) AND (4)	AC-2 (3) AND (4) AND (5) AND (11) AND (12)
	AC-3	Access enforcement		AC-3	AC-3	AC-3
	AC-4	Information flow enforcement		-	AC-4	AC-4
	AC-5	Separation of duties		-	AC-5	AC-5
	AC-6	Least privilege		-	AC-6 (2) AND (5) AND (9) AND (10)	AC-6 (2) AND (3) AND (5) AND (9) AND (10)
	AC-7	Unsuccessful logon attempts		AC-7	AC-7	AC-7
	AC-8	System use notification		AC-8	AC-8	AC-8
	AC-10	Concurrent session control		-	-	AC-10
	AC-11	Session lock		-	AC-11	AC-11
	AC-12	Session termination		-	AC-12	AC-12
	AC-14	Permitted actions without identification or authentication		AC-14	AC-14	AC-14
	AC-17	Remote access		AC-17	AC-17 (2) AND (3) AND (4)	AC-17 (2) AND (3) AND (4)
	AC-18	Wireless access		AC-18	AC-18	AC-18 (4) AND (5)
	AC-19	Access control for mobile devices		AC-19	AC-19 (5)	AC-19 (5)
	AC-21	Information sharing		-	AC-21	AC-21
	AC-22	Publicly accessible content		AC-22	AC-22	AC-22

		System and communication protection (SC)				
	SC-2	Application partitioning	Integrity	-	SC-2	SC-2
	SC-3	Security function isolation		-	-	SC-3
	SC-8	Transmission confidentiality and integrity		-	SC-8	SC-8
	SC-23	Session authenticity		-	SC-23	SC-23
	SC-28	Protection of information at rest		-	SC-28	SC-28
Media protection (MP)						
	MP-2	Media access	Integrity	MP-2	MP-2	MP-2
	MP-4	Media storage		-	MP-4	MP-4
	MP-5	Media transport		-	MP-5 (4)	MP-5 (4)
System and information integrity (SI)						
Integrity	SI-2	Flaw remediation		SI-2	SI-2	SI-2
	SI-3	Malicious code protection		SI-3	SI-3 (2)	SI-3 (2)
	SI-4	Information system monitoring		SI-4	SI-4 (2) (5)	SI-4 (2) AND (5)
	SI-5	Security alerts, advisories, and directives		SI-5	SI-5	SI-5
	SI-6	Security function verification		-		SI-6
	SI-7	Software, firmware, and information integrity		-	SI-7	SI-7 (2) AND (5)
	SI-8	Spam protection		-	SI-8 (2)	SI-8 (2)
	SI-10	Information input validation		-	SI-10	SI-10
	SI-11	Error handling		-	SI-11	SI-11
	SI-12	Information handling and retention		SI-12	SI-12	SI-12
	SI-16	Memory protection			SI-16	SI-16
	SC-5	Denial of service protection		SC-5	SC-5	SC-5
Physical and environmental protection (PE)						
Availability	PE-9	Power equipment and cabling		-	PE-9	PE-9
	PE-10	Emergency shutoff		-	PE-10	PE-10
	PE-11	Emergency power		-	PE-11	PE-11
	PE-12	Emergency lighting		PE-12	PE-12	PE-12
	PE-13	Fire protection		PE-13	PE-13 (3)	PE-13 (2) AND(3)
	PE-14	Temperature and humidity controls		PE-14	PE-14	PE-14
	PE-15	Water damage protection		PE-15	PE-15	PE-15
	PE-17	Alternate work site		-	PE-17	PE-17
	PE-18	Location of information system components		-	-	PE-18
	Contingency planning (CP)					
	CP-6	Alternate storage site		-	CP-6	CP-6

	CP-7	Alternate processing site	-	CP-7	CP-7
	CP-9	Information system backup	CP-9	CP-9	CP-9
	CP-10	Information system recovery and reconstitution	CP-10	CP-10	CP-10
Confidentiality	SC-4	Information in shared resources	-	SC-4	SC-4
	SC-10	Networks disconnect	-	SC-10	SC-10
	SC-12	Cryptographic key establishment and management	SC-12	SC-12	SC-12
	SC-13	Cryptographic protection	SC-13	SC-13	SC-13
	SC-17	Public key infrastructure certificates	-	SC-17	SC-17
	SC-19	Voice over internet protocol	-	SC-19	SC-19
	MP-3	Media marking	-	MP-3	MP-3
	MP-6	Media sanitization	MP-6	MP-6	MP-6 (2) AND (3)
	PE-5	Access control for output devices	-	PE-5	PE-5
	PE-16	Delivery and removal	PE-16	PE-16	PE-16
	IA-6	Authenticator feedback	IA-6	IA-6	IA-6
Confidentiality	SC-7	Boundary protection	SC-7	SC-7 (3) (4) (5)	SC-7 (3) AND (4) AND (5) AND (8) AND (18)
	SC-39	Process isolation	SC-39	SC-39	SC-39
	MP-7	Media use	MP-7	MP-7	MP-7
	PE-2	Physical access authorizations	PE-2	PE-2	PE-2
	PE-3	Physical access control	PE-3	PE-3	PE-3
	PE-4	Access control for transmission medium	-	PE-4	PE-4
	PE-6	Monitoring physical access	PE-6	PE-6	PE-6 (4)
CIA	SC-18	Mobile code	-	SC-18	SC-18
	SC-24	Fail in known state	-		SC-24

three baseline controls: *low-impact*, *moderate-impact*, and *high-impact*. NIST recommends to identify the baseline, determine the potential adverse impact for organizational information systems if there is a loss of confidentiality, integrity, or availability. Then, it introduces security controls for the three baselines.

We have extracted the technical controls to preserve CIA triad (the security goals) and categorized them based on the security goals they address, which we call *composed feature*. Table 2.1 represents the *Security Reference Model*. The first column reports the *cfs* which represents the security goals that the *afs* aim to address. Not implementing an *af*, will contribute to increases the likelihood of posing threat to the system, that is, *compromising the cf*. The second column reports the security controls identifiers. The control number (Ctrl#) defines the family of the control together with a unique number. The Third column lists the *afs*. If an *af* is not implemented, the related goal and consecutive goal, reported in fourth column, will be compromised. The last three columns represents the baselines for which an *af* is required; when the *af* is not required for a baseline the Table report it with a dash line. For example, *af* Authenticator management aim to preserve security goal *confidentiality* and, in consequence, security goal *integrity*. If it is not implemented, it contributes to increase the likelihood of threat *compromising confidentiality* and *compromising integrity*. Authenticator management control number is *IA – 5*, that defines the control is the fifth control belonging to Identification and Authentication family of control. NIST suggests to employ *IA – 5* for all three baselines.

For each security control, NIST defines *security control enhancements* that are used to supplement security controls. They are used in information systems and environments of operation requiring a greater protection than provided by the base control due to the potential adverse organizational impacts or when organizations seek additions to the base control functionality/specificity based on organizational assessments of risk. Therefore, to meet the minimum security for the system in question, the security control need to be implemented together with its control enhancements. Security control enhancements are numbered sequentially within each control. For example, *IA – 5* requires no security control enhancements for baseline *low*, while it requires for baseline *moderate* 2, 3, 4, 11 and *high* are 2, 3, 4, 8. To keep the Table simple, it does not contain the security control enhancements. Please refer to [NIS13], where they have listed them.

2.2.2 Privacy Reference Model

For data processing to be compliant, the controller needs to: (i) meet data processing principles, (ii) respect data subjects' rights and freedoms, and (iii) protect them from

risks to their rights and freedoms. As such the *Privacy Reference Model* has to cover them all.

Data Processing Principles. According to data processing principles, introduced in article 5.1, personal data shall be:

- processed lawfully, fairly and transparently (lawfulness and privacy goal *transparency*);
- collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with the purpose (privacy goal *purpose specification and limitation*);
- adequate, relevant and limited to what is necessary for the purposes of the processing (*data minimization*);
- accurate and, where necessary, kept up to date (*integrity*);
- kept no longer than necessary for the purposes of the processing (privacy goal *storage limitation*);
- processed in a manner that ensures integrity and confidentiality of data (security goal *integrity and confidentiality*).
- The controller shall be responsible for, and be able to demonstrate compliance with the above mentioned principles (*accountability*).

The privacy principles are aligned with privacy goals, introduced in Section 4.3; they are indicated in the parenthesis.

Data Subjects' rights and freedoms. Controllers shall facilitate the exercise of data subjects rights, articulated in article 15 to 22. For instance, the right to: data portability, rectification, and restriction of the processing. Privacy goal *interveinability* requires controller to facilitate the exercise of data subject rights (See Section 4.3).

Privacy Risks. Controllers need to ensure that data processing does not pose any risks to data subject's rights and freedoms. Surveying 43 information security and privacy experts, we learned that even experts confuse privacy risks with security risks (See Chapter 3).

There are security risks unrelated to privacy risks, just as there are privacy risks unrelated to security. Recognizing their boundaries is key to determine when security risk models and guidance may be applied to address privacy risks, and where gaps

Table 2.2: Mapping of Recital 75 Privacy Risks to Problematic Data Actions.

#	Recital 75: Privacy risk	Consecutive privacy risk	NIST: Privacy risk	NIST: Problematic data action
1	Discrimination	2, 9, 10, 4, 5	Discrimination	Distortion, Induced disclosure, Re-identification, Surveillance, Stigmatization, Unanticipated Revelation, Unwarranted Restriction
2	Financial loss/disadvantage	10	Financial loss	Appropriation, Insecurity, Unwarranted Restriction, Distortion
3	Reputation damage	10	Dignity loss	Insecurity, Re-identification, Stigmatization, Unanticipated Revelation
			Loss of liberty	Distortion, Surveillance
4	Exclusion	10	Loss of autonomy	Appropriation, Induced disclosure, Surveillance, Unanticipated Revelation
			Loss of Trust	Unwarranted Restriction, insecurity, Surveillance, Induced disclosure, Unanticipated Revelation, Re-identification, Appropriation
5	Physical harm		Physical harm	Surveillance
6	Identity theft	7, 8	Loss of trust	Unwarranted Restriction, insecurity, Surveillance, Unanticipated Revelation, Induced disclosure, Re-identification, Appropriation
7	Loss of confidentiality of personal data	10, 3, 1	Loss of trust	Unwarranted Restriction, insecurity, Surveillance, Unanticipated Revelation, Induced disclosure, Re-identification, Appropriation
8	Reveal of pseudonymization	7, 10, 3, 1	Loss of trust	Insecurity, Appropriation, Induced disclosure, Re-identification, Surveillance
9	Profiling	1, 2, 10	Discrimination	Induced Disclosure, Surveillance, Re-identification, Stigmatization, Unanticipated Revelation, Distortion
10	Social disadvantage	2	Loss of liberty	Distortion, Surveillance
			Discrimination	Induced Disclosure, Surveillance, Re-identification, Stigmatization, Distortion, Unanticipated Revelation
11	Revealing special category of personal data	1, 2, 3, 4, 5, 7, 8, 9, 10	Dignity loss	insecurity, Unanticipated Revelation, Stigmatization, Re-identification
			Discrimination	Stigmatization, Distortion, Re-identification, Unanticipated Revelation
			Loss of trust	Insecurity, Induced disclosure, Surveillance, Re-identification,
			Loss of autonomy	Unanticipated Revelation, Surveillance

exist [BGL⁺17]. Recital 75 introduces some privacy risks, such as: *loss of confidentiality of personal data*, *damage to reputation* and *financial loss*. While the former intersect with security risks and can be addressed by implementing security coun-

termes, there is no security countermeasure to address *damage to reputation*. Privacy risks are abstract notions and not easy to identify and address—unless you know the action that causes them and prevents the action. NIST calls such actions *problematic data action* [NIS20].

A *problematic data action* is a data action that causes an adverse effect, or problem, for individuals. In [NIS], NIST have introduced a *catalog of Problematic Data Actions and Problems*. The catalog lists problematic data actions and the *problem(s)*—which we call *privacy risks*—they could lead to. Appendix B defines the identified problematic data actions and their related privacy risks.

To address privacy risks, we need to prevent the problematic data actions that could cause them. As such, we have mapped the NIST introduced privacy risks to the ones introduced by Recital 75 to identify the problematic data actions that cause them. Table 2.2 shows the mapping. For example, *reputation damage* stated in recital 75 is mapped to *dignity loss* and *loss of liberty* introduced by NIST. A privacy risks can lead to other privacy risks, that we call *consecutive risk*. *Reputation damage* could lead to *social disadvantage*. This is captured by the second column of Table 2.2. A *problematic data action* could compromise a privacy goal(s). Table 2.3 lists this associations. Please note that, from this point on we refer to *problematic data action* as *privacy threat*; and that the association of some privacy risks to problematic data actions are debatable. For example, one can discuss that the problematic data action *surveillance* could not lead to privacy risk *discrimination*; while monitoring and tracking an individual could reveal much information about the person that could be used to discriminate him/her. Therefore, we have used the association recommended in *Catalog of Problematic Data Actions and Problems* by NIST [NIS20] as it is.

To this point, we have seen that privacy principles, rights and privacy threats are all to protect/compromise a privacy goal(s). Thus, we argue that meeting privacy goals can ensure that the data processing principles, data subjects’ rights, and privacy risks are addressed—that is to preserve data subjects’ rights and freedoms. In order to translate the privacy goals into concrete design requirements, we use privacy tactics. Section 4.4 has discussed the privacy tactics. Accordingly, we have built the *privacy reference model*, presented in Table 2.4. It comprises of three sections: (i) privacy threats, (ii) data processing principles, and (iii) data subjects’ rights; which are listed in the first column. The second column reports formulas which comprise of *afs* to meet the privacy goals, reported in third column. We devise the formulas considering the contribution of each *af* to meet a given privacy goal. We call the formulas $DPIA_{\text{privacy}}$. The last column reports the consecutive goals.

For example, privacy threat *induced disclosure* could compromise privacy goal *data minimization* and, in consequence, privacy goal *intervenability*. To prevent that, con-

Table 2.3: Mapping of Problematic Data Actions to Privacy Goals.

Problematic data action	Privacy goal
Distortion	Integrity
Induced disclosure	Data minimization
Re-identification	Unlinkability, Confidentiality
Stigmatization	Data unlinkability
Surveillance	Purpose specification Data unlinkability
Unanticipated revelation	Confidentiality
Appropriation	Purpose specification Transparency
Insecurity	Confidentiality Integrity
Unwarranted restriction	Transparency Intervenability

trollers could use privacy tactics `exclude` or `select` together with `choose`. `Select` requires to select only relevant people and attributes, and `exclude` requires to exclude irrelevant people or attributes in advance. Therefore, having one of them implemented is sufficient. While, `choose` offer users a real choice, which in the case of *induced disclosure* would be to give data subjects choice not to provide information disproportionate to the purpose. Accordingly, we have devised the formula. Privacy tactic `exclude` and `select` belong to a common privacy strategy, namely *minimize*. As such, they are enclosed within square brackets.

2.3 Formalization of Identified Problems

In this section we formalise the problems, namely P_{risk} and $P_{compliance}$, considering the reference models reported in Table 2.1 and 2.4.

Let $\mathcal{AF}$ be a set of *af*s (that refers to the extracted security control/privacy tactics to

Table 2.4: Privacy Reference Model.

	DPIA _{Privacy}	Composed Feature (Privacy Goals)	Consecutive goal
Privacy Threat			
Distortion	[obfuscate] AND [Restrict]	Integrity	confidentiality
Induced disclosure	[Exclude OR Select] AND Choose	Data minimization	Intervenability
Re-identification	[Mix OR Dissociate OR Obfuscate] AND [Summarize OR Group OR Perturb]	Data unlinkability	Confidentiality
Stigmatization			Purpose specification
Surveillance			Confidentiality
Unanticipated revelation			Confidentiality
Appropriation	[Consent] AND [Explain]	Purpose limitation	Transparency
Insecurity	[Mix OR Dissociate OR Obfuscate] AND Restrict AND [Distribute OR Isolate]	confidentiality and integrity	
Unwarranted restriction	Consent AND Choose AND Update AND Retract	Intervenability	Transparency
Threat to Data Processing Principle			
Compromising transparency	Supply AND Notify AND Explain	Transparency	
Unlawfulness	Create AND Maintain AND Uphold	Lawful process	
Unexpected purpose	Supply AND Notify AND Explain	Purpose specification	
Compromising data minimization	Exclude AND Select	Data minimization	Compliance
Unlimited storage	Destroy OR Strip	Storage limitation	
Compromising confidentiality and integrity	[Mix OR Dissociate OR obfuscate] AND Restrict AND [Distribute OR Isolate]	Confidentiality and integrity	
Unaccountability	Audit AND Report AND Record	Accountability	
Threat to Data Subjects' Right			
Infringing Right to access, portability and restrict	Consent AND Choose AND Update AND Retract	Intervenability	Compliance

protects the information system to satisfy a security/privacy goal(s)). We split the set in two disjoint subsets: $\mathcal{AF}_{\text{securityControl}} \cup \mathcal{AF}_{\text{PrivacyTactic}}$; Where $\mathcal{AF}_{\text{securityControl}}$ includes *afs* to meet security goals (listed in the third column of Table 2.1), and $\mathcal{AF}_{\text{PrivacyTactic}}$ includes the *afs* to meet privacy goals (listed in the second column of Table 2.4).

2.3.1 Problem P_{risk} definition

Let SA be a set of supporting assets that form the information system.

Let I be a set of implementation mappings whose elements are indexed over the set SA , such that an element $Impl_{sa}$ is in I if sa is in SA , and can take as input an af , to return a real value $Impl_{sa}(af)$ in the range $[0,5]$; when 0 indicates that there is no risk assigned to neither af nor sa , and any value higher than 0 indicates the likelihood of a related threat to either af or sa to occur.

Let ℓ be the likelihood level of compromising a given security/privacy goal. It is calculated by summing the likelihood level output by the $Impl_{sa}(af)$ function. Let p be the protection level for a given goal. It is calculated considering the number of implemented af .

Note that, the implementations of afs in $\mathcal{AF}_{PrivacyTactic}$ and $\mathcal{AF}_{securityControl}$ are *constrained* to them being *applicable* for the given data processing in question.

Let $\mathcal{G}$ be a set of goals and consecutive goals, listed in columns 1 and 4 of Table 2.1, and 3 and 4 of Table 2.4.

Let $\mathcal{T}$ be the set of threats and consecutive threats related to compromising the goal and consecutive goal when a given $\mathcal{AF}_{securityControl}$ is not implemented; and when a corresponding threat to a $\mathcal{AF}_{PrivacyTactic}$ poses. The threats are reported in the first column of Table 2.4.

We thus define the following mappings and relations:

- Let $AF2T$ be a relation between af of $\mathcal{AF}$ and its related threat(s).

The pairs in this relation can be defined by reading the elements reported in the third column of Table 2.1 and the second column of Table 2.4 and their related threat, indicated above.

- Let $T2G$ be a relation between each threat and its related goal.
- Let $T2CT$ be a relation between a threat and its consecutive threat.

The problem consists in finding afs and SA such that

$$\min_{Impl_{sa_1}, \dots, Impl_{sa_n}} \mathcal{R}(p, \ell, Impl_{sa_1}, \dots, Impl_{sa_n}, AF2T, T2G, T2CT) \quad (2.1)$$

subject to $sa_{1..n}$ is $\in SA$ and $af \in Appaf$, where SA is a set of supporting assets required to conduct the data processing in question, and $Appaf$ is a set of applicable af to protect security and privacy of SA .

$\mathcal{R}$ is thus an operator that returns the risk level given the I, $Appaf$ and calculated the protection and likelihood level. In our case, $\mathcal{R}$ is instantiated with the procedure supported by the RiskML tool (explained in Section 4.5). First, this allows the controller to perform a risk assessment taking into account the risk propagation, namely the propagation of the negative effects of the threats and the positive effects of the implemented $Appaf$. Second, RiskML support a trade-off analysis, allowing the controller to consider the risk associated with each choice.

2.3.2 Problem $P_{compliance}$ Definition

Let us define a complex proposition as a formula obtained from af in $\mathcal{AF}$ and logical connectives.

Let us call $DPIA_{security}$ and $DPIA_{privacy}$ the set of complex propositions reported in the *Baseline* column of Table 2.1, and second column of Table 2.4, respectively. When a complex proposition is satisfied, it returns 1, and 0 otherwise.

Let us call $\mathcal{AF}_{baseline}$ a set of af related to the baseline control to which the data processing belongs.

We thus specify the problem $P_{compliance}$ of compliance with regards to DPIA requirements of security and privacy: given the set of $DPIA_{security}$ and $DPIA_{privacy}$, we state that an information system complies with the security requirements of DPIA when the Boolean mapping of implemented $Appaf$ satisfies all the complex propositions in the $DPIA_{security}$ related to the $\mathcal{AF}_{baseline}$ of the information system in question; and complies with the privacy requirements of DPIA when the Boolean mapping of implemented $Appaf$ satisfies all the complex propositions of the $DPIA_{privacy}$.

Note that, as mentioned, the $DPIA_{security}$ and $DPIA_{privacy}$ can be updated according to the context, that is, introducing the security/privacy reference model that suit best the information system.

Chapter 3

Can Data Subject Perception of Privacy Risks Be Useful in a DPIA?¹

People engage in online activities to gain psychological [TM12], emotional [KKVG11], economical or social benefits, while an increasing number of critics have voiced their concerns over privacy [KK12, GRV19, BMA94] and social welfare [ATW16]. People are rightly concerned about the commercial exploitation of their personal data [ATW16]. The GDPR [GDP16] was introduced to protect natural persons concerning the processing of their personal data. GDPR requires to conduct a DPIA whenever there are high risks to data subjects' rights and freedoms. DPIA provides some indications on when the impact of a risk is high, e.g., when new technologies are used—the list is non-exhaustive.

DPIA asks to seek data subjects' perception where appropriate (article 35.9). However, (a) people are not aware of privacy risks (as discussed in [GRV19, SV14]), and (b) their perception can change in different contexts [VSSJJ06, MDMÖG18, CNI12b]. Given people's unawareness of privacy risks, *we aimed to assess their privacy risk perception when given awareness (RQ1)*.

Identifying risks to data subjects' rights and freedoms might not be easy for experts, as it is a new perspective. Given DPIA's perspective on privacy risks and the importance of identifying the boundary of privacy risks with security risks [BGL⁺17]; *we also aimed to examine whether security and privacy experts can differentiate privacy risks from security risks (RQ2)*.

To this end, we have conducted two surveys: *Guided Survey* and *Unguided Survey* to address RQ1 and RQ2, respectively. The surveys considered a scenario to get people

¹The work is published in [DSDOK⁺21]

into a certain mindset [HFS14], while avoiding bias. The *Guided Survey* listed 20 privacy risks and asked participants to evaluate their impact, while the *Unguided Survey* asked security and privacy experts to identify and evaluate five privacy risks related to the scenario.

Findings. The *Guided Survey* showed that awareness helps participants better estimate privacy impact when using correct communication; age and context influence people’s perception. The *Unguided Survey* showed that experts confuse security risks with privacy risks.

Plan of the Chapter. Section 3.1 discusses quantitative analysis. Section 3.2 discusses our research questions and the steps we took to conduct the surveys. Section 3.3 shows the results, and Section 3.4 further discusses them. Section 3.5 gives a brief insight into related studies, and Section 3.6 concludes the chapter.

3.1 Background: Quantitative Analysis

To draw valid conclusions we quantitatively analyzed the results of surveys. The quantitative interpretation has three steps: *descriptive statistics*, *data set reduction* and *hypothesis testing* [WRH⁺12]. The first step deals with the presentation and numerical processing of a data set. We have used a plot and tables to present our collected data. The second step is to clean the data. The data we collected from the *Guided Survey* was clean as it was a multi-choice form. While the *Unguided Survey* had open answers and required to be cleaned; some of the answers were long and descriptive, while others were short and to the point. To ease the process of analysis, we applied the Intercoder reliability solution presented in [Kur00], that is, an agreement to proxy the validity of the constructs that emerge from the data in a systematic way. We elaborate on this in Section 3.3.2. The last step is the statistical evaluation to verify whether we should reject the null hypothesis (H_0), with a certain significance level, in favour of the alternative hypothesis (H_a). A H_0 states that there is no difference between certain characteristics of a population, while H_a proposes that there is a difference. The *significant level* α is the highest *p-value* we accept for rejecting H_0 . A typical value, inherited from widespread practice is $\alpha = 0.05$; which we have also considered in our test. The *p-value* denotes the probability of rejecting H_0 when it is true.

Hypothesis tests are classified into *parametric tests* and *non-parametric tests*. The former assumes that the population is normally distributed, while the latter does not make any assumption. Generally, hypothesis tests can be either *one-sided* or *two-*

sided. This distinction governs whether the test has a rejection region located in one (*one-sided*) or both tails (*two-sided*) of the distribution. We make no assumption on the underlying distribution of the data we have collected. Moreover, we wanted to check if the estimations are above a certain value. Therefore, we used the one-sided Wilcoxon Signed Rank Test for a median. The description on the Quantitative interpretation and hypothesis test follows [WRH⁺12].

3.2 Motivation and Methodology

Surveys, case studies and experiments are all different types of investigations that serve a specific purpose. We used surveys to collect people’s attitudes [WRH⁺12]. However, [HFS14] states that asking people about past behavior causes biases, while using a scenario-based survey gets people into a certain mindset before eliciting their attitudes within that mindset. As such, we introduced the scenario.

Studies (see e.g., [GRV19, SV14]) showed that lay people are not aware of privacy risks. Fischhoff et al. [FSL⁺78] state that risk perception decreases if risks are perceived as either voluntary, not immediate, controllable or when using available technologies. For example, social networks are perceived less risky as they are known technologies [GRV19]; people voluntarily reveal their sensitive information², such as sexual experiences, religion and political opinions [WNK⁺11, DFKA⁺20]—for which GDPR requires a higher level of protection. Another example is online banking or e-commerce services that are perceived risky [SYF18] due to their immediate impact. We wanted to have a combination of the above-mentioned aspects. As such, we presented participants with a fictitious online social network that provides intimate dating service: known and widely used technology [Cha17, BN18, PPHR20], while having immediate impacts [LB12].

People’s privacy unawareness [ANG17, HFS14, ZMR17] could be due to the way they inform themselves, e.g., by listening to stories or media. Indeed, authors in [SYF18] suggest this as an explanation for people’s top three privacy risks: identity theft, account breach, and job loss. To raise awareness, authors in [GRV19] and [DFKA⁺20] have warned participants by bringing the possible privacy risks in the context of their scenario. For example, the former asks participants to estimate the impact in the following scenario “Your entered data [...] are analyzed by the various Smart Home manufacturers [...] It is known where you are at what time. That way you can become a victim of stalking”. Although we wanted to examine whether awareness raises concern of lay people, we wanted to avoid bias by not introducing related privacy risks in the context of the scenario, as in mentioned studies. People’ risk

²<https://www.kaspersky.com/blog/online-dating-report/>

perception is higher if they can relate, e.g., losing a job due to data sharing on Facebook [GC13]. Thus, we raise awareness in the opening lines of our surveys by giving the example of Facebook–Cambridge Analytica data scandal³. This is to challenge people’s perspective by indicating that known technology are not necessarily less risky.

We designed two online scenario-based surveys, namely *Guided Survey* and *Un-guided Survey*. The former asked participants to estimate the impact of listed privacy risks, while the latter asked them to identify related privacy risks to the scenario. Before running the *Guided Survey*, we conducted an internal *Pilot Survey* to examine the *Guided Survey*. We took the privacy risks listed in *Guided* and *Pilot* surveys from the CNIL *Knowledge base* [CNI12b] document. The document lists 64 damages, called *feared events*, and provides examples of an impact estimation for each. A feared event is “a breach of personal data security likely to have impacts on data subjects’ privacy” [CNI01b]. Feared events have been referred to in literature by different terms; in this paper, we use the term *privacy risk*.

Impact estimation is on a scale of 1 (negligible) to 4 (maximum), where 1 means have no concern and 4 means very concerned. The surveys were designed and responded to in English; and were conducted from mid-October 2019 until the end of February 2020.

Research Questions. The DPIA under the GDPR is a tool for managing risks to the rights of the data subjects, and thus takes their perspective; conversely, risk management in other fields (e.g. information security) is focused on the organization[Arta]. It requires, where appropriate, to seek data subjects’ perceptions. People are not aware of privacy risks [SV14, GRV19], however social awareness is a predictor of privacy risks [DH06]. Given the awareness warning we raised with the opening line, our first research question is:

RQ1: How do lay people perceive privacy risks?

DPIA is concerned with data subjects’ rights and freedoms. That is a new perspective for information security and data privacy experts. Although, security and privacy domains intersect, recognizing their boundaries is key to determine when security risk models and guidance may be applied to address privacy risks and where gaps exist [BGL⁺17]. For instance, the *profiling and automated decision making* is not a security risk, while according to article 35, it is kind of processing that is likely to result in a high risk to the rights and freedoms of natural persons. If experts fail

³https://en.wikipedia.org/wiki/Facebook-Cambridge_Analytica_data_scandal

to identify and assess privacy risks correctly, organizations may fail to comply with GDPR. As such, our second research question is:

RQ2 : Can information security and data privacy experts distinguish security risks from privacy risks?

Procedure. The *Guided Survey* and the *Pilot Survey* consist of 9 pages, whereas the *Unguided Survey* has 5 pages. The first three pages and the last page of the surveys are the same. The first page contains the opening lines, the aim of the study, the procedure, the estimated completion time for the survey, and the privacy statement. The second page asks participants to specify their age range. The third page provides the scenario, and the last page thanks to the participants. We have included these pages in Appendix [A.1](#).

- *Pilot Survey.* From page four to eight, each page asked participants to choose a privacy risk from a given list. The list contains 64 privacy risks. They needed to determine the likelihood, impact, and treatment(s). According to the feedback and our observations, we updated the *Guided Survey* as follows:

1. kept only 20 privacy risks out of 64. To select the risks, we had three principles:
1) being related to the scenario, 2) being distinct, and 3) picking from all impact levels (from negligible to maximum);
2. removed likelihood estimation since perceived privacy risk is not the product of likelihood and impact, as observed in [\[BB18\]](#);
3. categorized risks into five groups based on the specific consequences, to increase readability, inspired by [\[KTTV17\]](#): *Discrimination/Manipulation*, *Financial loss*, *Social disadvantage*, *Deprived to exercise rights*, and *Physical harm*. Each group has four privacy risks (See the first two columns of Table [3.1](#));
4. simplified the text of two privacy risks to avoid confusion: *invasion of privacy* and *psychological problem*.

Six of the privacy risks mentioned in the CNIL knowledge base document [\[CNI12b\]](#) address two privacy risks with different levels of impact. Three of them refers to *feeling of invasion of privacy*, which are:

1. *feeling of invasion of privacy without real or objective harm*, with impact level *negligible*;

2. *feeling of invasion of privacy without irreversible damage, with impact level limited; and*
3. *feeling of invasion of privacy with irreversible damage, with impact level significant;*

and other three refer to *psychological ailments*, which are:

- *minor but objective psychological ailments (defamation, reputation), with impact level limited;*
- *serious psychological ailments (e.g., depression, development of a phobia), with impact level significant; and*
- *long-term or permanent psychological ailments, with impact level maximum.*

We learned that the above mentioned privacy risks confused participants. Thus, as the point number 4 indicated, we have instead used *feeling of invasion of privacy* and *psychological problem (e.g., development of a phobia, loss of self-esteem)*.

- *Guided Survey.* From page four to eight, each page demonstrates a category of risk. Each category contains four privacy risks (see Table 3.1). For instance, the first category is *Discrimination and manipulation risk*, which contains the following four risks: (1) Targeted, unique and nonrecurring, lost opportunities (e.g., refusal of studies, internships or employment, examination ban); (2) Feeling of violation of fundamental rights (e.g. discrimination, freedom of expression); (3) Targeted online advertising on a private aspect that the individual wanted to keep confidential (e.g., pregnancy advertising, drug treatment); (4) Inaccurate or inappropriate profiling. The survey asked participants to estimate the level of impact each privacy risk could have in the case of a data breach. We have included these pages in Appendix A.2.

- *Unguided Survey.* Page four of the survey contains five text boxes and asked participants to identify five privacy risks. For each, they are asked to evaluate their impact and introduce relevant applicable treatment to address the identified privacy risks. We have included it in Appendix A.3.

Recruitment and Participants. For the *Pilot Survey*, we reached out to our colleagues at SAP⁴, from unrelated centers to the field of information technology, in particular to information security and data privacy. The survey received 21 responses with all questions answered.

⁴<https://www.sap.com>

For the *Guided Survey*, we reached out to our colleagues, at Bruno Kessler Institute⁵ from unrelated centers to the field of information technology, in particular to information security and data privacy. Additionally, responses were from Bachelor's and Master's students at the University of Trento⁶ in the physics and mathematics department of our university. The survey received 88 responses with all questions answered.

For the *Unguided Survey* we reached out to our colleagues who work on information security and data privacy at the Bruno Kessler Institute⁵ and SAP⁴. The survey had 43 responses with all questions answered.

Note that, to avoid biases we did not use incentive-based approaches [LHP⁺19] to ensure that the participants participate voluntarily and avoid impacting who participates [HK16].

Ethics. Ethical preconditions given for research involving personal data by our companies's ethics committee were met. The first page informed participants about the purpose and procedure of the survey. They are informed that they can choose not to continue the survey at any time during the study without providing a reason. The identities of the respondents are not collected. We have no means to link the individual answers to any given respondent. The participants' responses are stored privately and only the responses only used for research purposes.

3.3 Results

Below, we report the results of the two surveys. The raw data collected from both surveys can be find in [raw].

3.3.1 Results of Guided Survey

The *Guided Survey* answers *RQ1* that examines lay people's perception of privacy risks given an awareness warning. We considered impact higher than 2 (limited) to be high, which is either 3 (significant) or 4 (maximum). Accordingly, we have formulated the H_0 as "lay people's impact estimations are equal or lower than 2", and H_a as "lay people's impact estimations is greater than 2". Table 3.1 shows the test results and the frequency of given impact by participants. For instance, the

⁵<https://www.fbk.eu/en/>

⁶<https://www.unitn.it/en>

Table 3.1: Guided Survey Result.

Category	Privacy Risks	Impact level Frequency				P-value	H0	Ha
		#1	#2	#3	#4			
Discrimination	Targeted, unique and nonrecurring, lost opportunities (e.g., refusal of studies, internships or employment, examination ban)	12	18	37	21	0	Reject	Accept
	Feeling of violation of fundamental rights (e.g. discrimination, freedom of expression)	1	13	40	34	0	Reject	Accept
/Manipulation	Targeted online advertising on a private aspect that the individual wanted to keep confidential (e.g., pregnancy advertising, drug treatment)	4	21	26	37	0	Reject	Accept
	Inaccurate or inappropriate profiling	3	24	40	21	0	Reject	Accept
Financial loss	Non-temporary financial difficulties	12	26	29	21	0	Reject	Accept
	Unanticipated payment	7	30	27	24	0	Reject	Accept
	Missing career promotion	13	26	30	19	0	Reject	Accept
	Financial loss as a result of a fraud (e.g., after an attempted phishing)	5	18	28	37	0	Reject	Accept
Social Disadvantage	Loss of family tie	20	23	21	24	0	Reject	Accept
	Separation or divorce	29	18	21	20	0.0044	Reject	Accept
	Receipt of targeted mailings likely to damage reputation	9	23	33	23	0	Reject	Accept
	Cyberbullying and harassment like blackmailing	10	11	27	40	0	Reject	Accept
Deprived to exercise right	Losing control over your data	0	13	37	38	0	Reject	Accept
	Reuse of data published on websites for the purpose of targeted advertising (information to social networks, reuse for paper mailing)	2	7	30	49	0	Reject	Accept
	Feeling of invasion of privacy	6	5	31	46	0	Reject	Accept
	Blocked online services account (e.g., games, administration)	12	27	34	15	0	Reject	Accept
Physical harm	Psychological problem (e.g., development of a phobia, loss of self-esteem)	19	24	19	26	0	Reject	Accept
	Defamation resulting in physical retaliation	21	21	31	15	0.0001	Reject	Accept
	Physical issues like transient headaches	29	34	17	8	0.5131	Accept	Reject
	Alteration of physical integrity, e.g., following an assault, an accident at home, work, etc.	24	35	18	11	0.1055	Accept	Reject

LEGEND. #1: Frequency of Negligible, #2: Frequency of Limited, #3: Frequency of Significant, #4: Frequency of Maximum

frequency of negligible (value 1) for privacy risk *Losing control over one's data* is zero, for limited (value 2) is 13, for significant (value 3) is 37 and the frequency of maximum (value 4) is 38. In this case, the H_0 is rejected in favor of H_a . The results show that participants have high concerns about privacy risks, except for privacy risks "Physical issues like transient headaches" and "Alteration of physical integrity, e.g., following an assault, an accident at home, work, etc."

Different factors influence people's perception of privacy; age is one of them, as stated in [WZ11, You09]. We wanted to examine this statement. The age distribution of participants to the Guided Survey is the following: 35 (39.78%) are aged 18 – 24

Table 3.2: Age Range Impact Analysis for Privacy Risks that Accept the H_0 .

Privacy Concerns	P-Value	age 18 to 25	P-Value	25 to 34	P-Value	35 to 54
Loss of family tie	0.2735	Accept	0.004	Reject	0.0002	Reject
Separation or divorce	0.7747	Accept	0.0906	Accept	0.0003	Reject
Psychological problem	0.0008	Reject	0.2029	Accept	0.0015	Reject
Defamation resulting in physical retaliation	0.0388	Reject	0.1509	Accept	0.0006	Reject
Physical issues like transient headaches	0.4216	Accept	0.4153	Accept	0.7561	Accept
Alteration of physical integrity, e.g., following an assault, an accident at home, work	0.1006	Accept	0.384	Accept	0.305	Accept

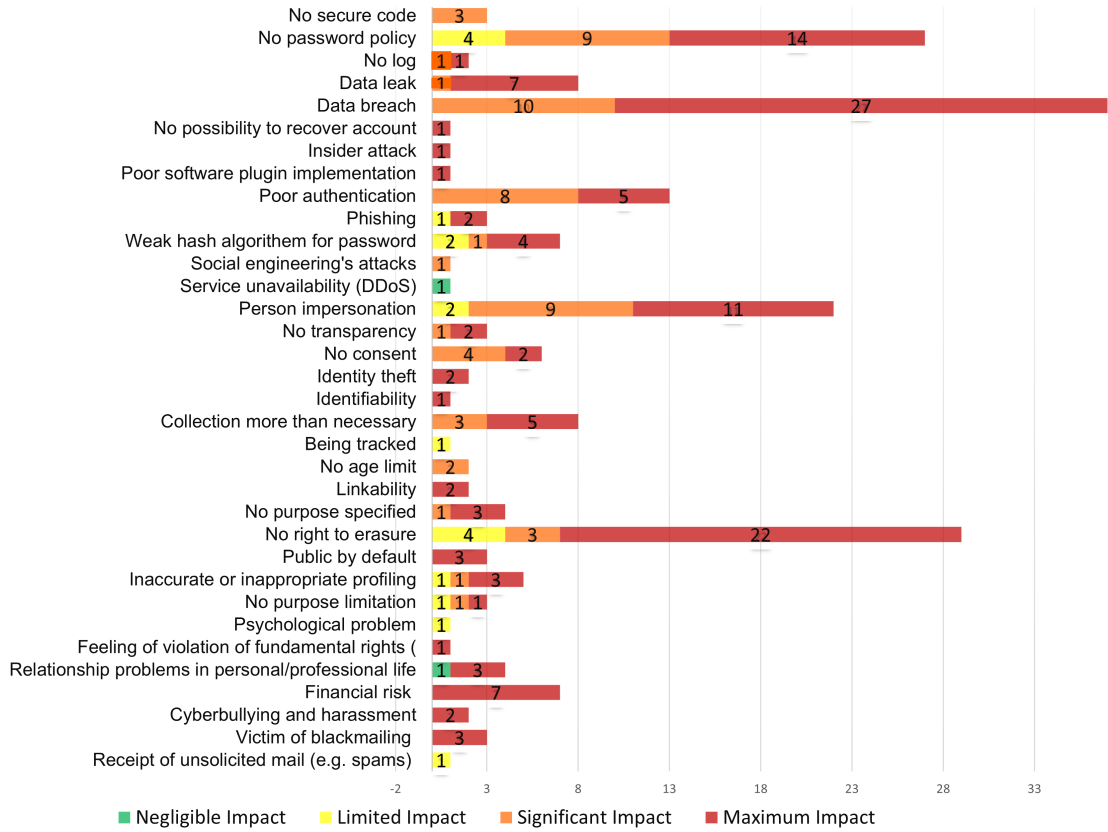


Figure 3.1: The Identified Privacy risks With the Frequency of Given Impacts.

years, 29 (45.45%) are aged 25 – 34 years, 12 (12.5%) are aged 35 – 44 and 12 (2.27%) are aged 45 – 54. Table 3.2 lists only the privacy risks where at least one of the age ranges accept the H_0 ; for the rest, all agreed to reject the H_0 . Since the samples from the age range 35 – 44 and 45 – 54 were too small, we consider the age range 35 – 54 as a single bin. The results show that age range 18 – 24 has less concern about the privacy risk *Separation and divorce* and *Loss of family tie*. The age range 25 – 34 also has low concern about the former and have no concern about *physical* and *Psychological harms*. While age range 18 – 24 and 35 – 54 have higher concern about *Psychological problem* and *Defamation resulting in physical retaliation*.

3.3.2 Results of Unguided Survey

The *Unguided Survey* answers *RQ2* that assesses whether information security and data privacy experts can appropriately distinguish privacy risks from security risks. We did not run the statistical test on the *Unguided Survey*, as the samples were

small for each identified risk. For example, the privacy risk *collection more than necessary* was identified 8 times only (See Figure 3.1).

Figure 3.1 lists all the identified risks. The numbers on the bars indicate the frequency of the given impact level. For example, *No password policy* has been identified 27 times: 4 times with *limited* impact, 9 times with *significant*, and 14 times with *maximum* impact level. The privacy/security text presented in the Figure are after applying the Inter-coder reliability solution [Kur00]. Our principles to annotate, where possible, were to use either: (1) the same text as the CNIL, e.g., *cyberbullying* and *financial loss*; (2) the texts used in literature, e.g., *identifiability* and *unlinkability*; or (3) the GDPR principles e.g., *no transparency*, and *no purpose limitation*. For example, “There is no user’s consent to store user’s data. User is not informed which type of data are stored”, is annotated as *no consent* and *no transparency*. We have also deleted four irrelevant answers, e.g., *No idea*. The participants have identified 34 issues when 21 of them are privacy risks, indicated with the solid-border rectangle, and the rest are security risks. Participants were within the age range of 30 to 44.

3.4 Discussion

This section discusses the analysis of the results for the surveys (Section 3.4.1 and 3.4.2).

3.4.1 RQ1: People’s Perception

The first research question aims to assess lay people’s perception of privacy risks in the context of a scenario when given an awareness warning. As Table 3.1 showed, except for two privacy risks related to *Physical harm*, H_0 is rejected in favor of H_a that is, *lay people’s impact estimations is greater than 2*. The results fulfilled our expectation.

Authors in [LB12] discussed that, among 14 surveyed scenarios, people consider *viewing adult content and online dating* to lead to embarrassment and accordingly evaluated it to have a high impact. However, other works with different/no scenarios confirm our results. We have compared the impact of common privacy risks in the *Guided Survey*, listed in Table 3.3, with the related risks in the following scenario-based works [LB12, HFS14, GRV19, BHS⁺16, MDMÖG18]; and three years of the Special Eurobarometer general surveys which reach more than 20,000 peo-

Table 3.3: Impact Estimations of Same Privacy Risks By Different Works.

Privacy Risks	Guided Survey	Other Works
Losing control over one's data	Maximum (35.23%) Significant (40.91%)	[EU2011]: 78% (out of 26,574) feel to have no or partial control. [EU2015]: 67% (out of 16,244) concerned to have no control. [EU2019]: 78% (out of 15,915) concerned to have no control.
Reuse of data published on websites for the purpose of targeted advertising (information to social networks, reuse for paper mailing)	Maximum (44.32%) Significant (34.9%)	EU2011: 70% (out of 26,574) secondary purposes concern. EU2015: 69% (out of 27,980) secondary purposes concern. [Mohallick et al., 2018]: secondary purpose is the main concern.
Targeted online advertising on a private aspect that the individual wanted to keep confidential (e.g., pregnancy advertising, drug treatment)	Maximum (40.90%) Significant (30.68%)	EU2011: 54% (out of 26,574) significant to maximum concern. EU2019: 53% (out of 21,707) significant to maximum concern.
Inaccurate or inappropriate profiling	Maximum (25%) Significant (44.32%)	[Bellekens et al., 2016]: categorized them as the most impactful.
Financial loss as a result of a fraud (e.g., after an attempted phishing)	Maximum (40.91%) Significant (31.82%)	[Gerber et al., 2019; Bellekens et al., 2016, Harbach et al., 2014, LeBlanc and Biddle, 2012]: financial is impactful.
LEGEND. EU2011: [Special Eurobarometer 359, 2011], EU2015: [Special Eurobarometer 431, 2015], EU2019: [Special Eurobarometer 487a, 2019]		

ple, from 2011⁷ [Spe11], 2015⁸ [Spe15] and, 2019⁹ [Spe19]. For instance, privacy risk *inaccurate or inappropriate Profiling* perceived to have a significant impact by 44.32% of lay people participated in *Guided Survey*, and to be the most impactful by [BHS⁺16]. Moreover, Solove in [Sol20] suggests people care about their privacy; they behave according to the context. He argues that it does not mean that they are unwilling to share their personal data but rather evaluate advantages and disadvantages to take a calculated risk. That contradicts with the works that state lay people tend to base their decisions on personal experiences rather than real concerns, such as [ZJ16, DJ16, Sch06, TSR11]. The cases where people seem to be unaware or not being concerned about their privacy could be due to how they inform themselves, e.g., by listening to stories or media. Indeed, authors in [SYF18] suggest this as an explanation for people's top three privacy risks: identity theft, account breach, and job loss. Authors in [GRV19] discussed that people underestimate abstract risk scenarios compared to specific scenarios where the method by which data can be abused is described. Therefore, risk communication matters to reduce, if not close, the gap between perception [SYF18, TSR11] and reality. The first step towards achieving this goal is to assess how people perceive privacy risks by describing either general potential harm or negative consequences, using an intelligible language [GRV19]. The authors of [Cam09] argue the use of physical and criminal metaphors in security risk communication, which could also be applicable for privacy risks. [GC13] suggests using examples that are easy to recall, such as losing a job due to data sharing on Facebook. One can argue that because of the paradox concerning misalignment between people's privacy attitude and privacy behaviour [NHH07], only assessing data subjects' perceptions might not be enough;

⁷It explores citizen's attitudes concerning identity management, data protection and privacy.

⁸It explores how people feel over the personal data they provide online.

⁹It explores awareness of GDPR in particular, and opinions on data sharing and data protection.

their behavior should be examined to prove the accuracy of claims [Pre13]. However, Solove suggests that there is no paradox [Sol20] because people take context-aware decisions about accepting certain risk levels.

The result also showed that people of different ages have different concerns about *loss of family tie* and *separation and divorce* (see Table 3.2). Some works (see e.g., [SDX11]) also show that *age* influences people’s perception, while some others [MDMÖG18, VSSJJ06] did not find any significant difference across age groups. According to our results, it depends on the privacy risk category under consideration and cannot be generalized.

The answer to *RQ1* is that raising awareness while avoiding bias, does help lay people to understand the impact of privacy risks better when unambiguous language and concrete examples are used. As context influences peoples’ perceptions, controllers should not use the result of an existing data processing without considering the context.

3.4.2 RQ2: Experts’ Perception of Privacy Risks

The second research question aims to understand whether information security and privacy experts can distinguish privacy risks from security risks. Figure 3.1 shows that the participants have identified 34 issues, among which 21 are privacy risks. Given that the participants are explicitly asked to identify privacy risks, the answer to *RQ2* is that experts confuse them with security risks. Recognizing the boundary of security and privacy risks is the key to determine when security risk models and guidance may be applied to address privacy risks, and where there are gaps [BGL⁺17]. That can result in misjudging either the necessity of the DPIA or the impact level of data processing on data subjects. Controllers may want to collaborate with legal fellows and Data Protection Officers. It is also good practice to use tools that can guide to identify privacy risks (see, e.g., [DR20a]).

3.5 Related Work

Rapid technological developments significantly increased and took over our daily lives. The scale of collecting, sharing, and processing of personal data challenges organizations to protect personal data, especially related to concerns regarding individual privacy [ACR99, Kob01, AEY10, CRA00, OGH05, Pre13]. The data is not the problem; it is who gets to see and use those data, which creates problems [RD16]. The number of breached records jumped significantly in 2019, with over 8.5 billion

records exposed—more than three times greater than 2018. ¹⁰

Warren and Brandeis defined privacy as “[the] right to be let alone” [WB90]. This definition evolved over time: “personal adjustment process” (1967) [Wes67]; “boundary regulation process whereby people optimize their accessibility along a spectrum of *openness* and *closedness* depending on context” (1975) [Alt75]; “a fundamental right, essential for freedom, democracy, psychological well-being, individuality, and creativity” (2008) [Sol08]. The General Data Protection Regulation (GDPR) [GDP16] states that the protection of natural persons concerning the processing of personal data is a fundamental right.

A Privacy Impact Assessment (PIA), developed in the 1990s, is an instrument to safeguard privacy [WdH12]. D.Wright defines PIA as “a methodology for assessing the impacts on the privacy of a project, policy, program, service, product or other initiatives which involves the processing of personal information and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimize negative impacts” [WdH12]. PIA has been largely studied by academic [Cla09, Wri12, OS14, Cla99, Spi12, CK13, SWBS19, ACDC⁺15, VK18, ASRJ18, OS14] and data protection authorities [CNI01c, CNI01b, CNI01a, ICO14]. However, PIA has not been a mandatory assessment. Article 35 of the GDPR introduced Data Protection Impact Assessment (DPIA) and made it mandatory whenever the type of data processing is likely to result in a high risk to the rights and freedoms of natural persons. The DPIA focuses on data protection, unlike the PIA, which protects all types of privacy [WFR13]. Still, some literature criticises the DPIA for being too limited in scope [WFR13].

Article 35(7) provides only a minimum standard for carrying out the DPIA without further explanation. Thus, data protection authorities and academics introduces guidelines and tools to help controllers conduct the DPIA [CNI01c, ICO18, Arta, BFH⁺16, CFKA18, ASRJ18, SWBS19, ACDC⁺15, DR20a].

The GDPR protects data subjects against any risks to their rights and freedoms concerning processing their data. It lists, in recital 75, some example damages that are risks to data subject’s rights and freedoms. Literature has largely studied privacy risks [DLM16, SC08, OS14, Sol05, NIS]. Some studies focus one particular privacy concern, e.g., profiling [TWC12], tracking [Rad14], and identity theft [JKN⁺20], while some other studies focus on a specific domain, e.g., recommender system [MDMÖG18]; internet of things [ZMW14]; and eHealth [BHS⁺16]; online multimedia collection [CM07] Social Networks, smart home, and smart health devices [GRV19], crowd-sourcing [XM20]. Some others study privacy concerns in more general contexts [Spe11, Spe15, Spe19, SV14, GCCLH12, OL08].

¹⁰<https://www.ibm.com/security/data-breach/threat-intelligence>

Different factors influence people's perception of privacy concerns, such as: cultural background and demography [VSSJJ06, MDMÖG18, SDX11, Sta69, GRV19, BG⁺10, BB18, KVG12]; person's own values, general perceptions, and experiences [BPJR07]; data type, data recipient, and data purpose [Nis09]. The author in [FSL⁺78] stated that an individual perceives a concern more severe if it is: involuntary (also mentioned by [Sta69]), has an immediate effect, unknown risk, unknown science, uncontrollable, chronic/catastrophic risk, and uncommon-dread. Some studies suggest that age and gender did not influence their results [MDMÖG18, VSSJJ06], while others observed the influence [WZ11]. Additionally, some studies focus on the relation between online privacy concerns and different ages (see, e.g., [You09]). Indeed, our *Guided Survey* results suggest that age influenced participants' perception.

Different data actions upset different people: being tracked and profiled by targeted ads while browsing online [WXH16], the way social media platforms process personal data [WNK⁺11], online dating [GEL11] and drone surveillance [WXYH16].

It is essential to identify and understand the various kinds of socially recognized privacy concerns [Sol05]; and ultimately to accurately estimate their impact level. Experts and lay people evaluate privacy concerns differently. Lay people tend to judge based on their past experiences [ZJ16, DJ16] or on perceived concerns rather than real concern [Sch06, TSR11]; they are not aware of specific privacy concerns [SV14]. For example, people either do not correlate privacy concerns with issues related to identification and tracking or if they do, they believe it would be to produce personalized advertisements [SV14]. Whereas experts judge based on the objective probability and severity of a concern [ZJ16, DJ16]. Sometimes, when people's benefits outweigh privacy concerns, there is a mismatch between people's privacy attitudes and behaviour. This situation is called the privacy paradox, and it can result in severe misjudgments [ANG17, ZMR17, HFS14, GRV19]. Therefore, it is necessary to reduce, if not close, the gap between people's perception and the real concern [SYF18, TSR11].

The first step is to assess how people perceive privacy risks by communicating about the possible harms and their consequences. Findings of a survey [GC12] suggest that risk communication contextualizes risks that may be too abstract for a non-expert user, thereby reducing the psychological distance to the risk and altering the perceived severity. Investigating into the type of thinking users engage in can provide valuable insights for usable privacy research [CG14]. The author in [Cam09] suggest that mental models are the proper way to communicate risks. Some projects have already adopted them: Primelife project form mental models of data minimization property of the concept of anonymous credentials [Pet08]; Analogies and metaphors help to structure an unfamiliar domain and provide guidance to support notice and support [LMD03]; Audience-view [LBW08] metaphor has been

proposed to Facebook users to form a model of their data recipients. The author in [Pre13] acknowledges the paradox and concludes that it is necessary to measure both behaviour and attitude in their own right, and with their specific procedures. The GDPR requires seeking peoples' views when appropriate. Due to the privacy paradox, we suggest to both seek their view and examine their behaviour. Experiments can investigate the validity of the claims, while surveys collect information from or about people to describe, compare or explain their knowledge, attitudes and behaviour [WRH⁺12].

Engineers see privacy issues as: an abstract problem, not an immediate problem, not a problem at all, not their problem, or simply not part of the project deliverable [LLR05]. In contrast, privacy-conscious engineers strive for extremely high degrees of privacy protection [SC08] that undermine system usability [DM05]. Our survey results, see Section 3.4.2, also suggest that information security and privacy experts confuse security risks with privacy concerns. They need to be guided and collaborate with legal fellows.

3.6 Conclusion

This chapter presents the results of two scenario-based surveys: *Guided* and *Unguided*. The *Guided Survey* investigated people's perception of privacy concerns when giving them an awareness warning about privacy risks beforehand. Analyzing its results, we observed that: (i) although awareness helps people to perceive privacy risks better, the language used to communicate risks matters—less vague and more familiar risk examples are better; (ii) age impacts on how one perceives a given privacy risk; (iii) context impacts on privacy risks' perception, which highlights the fact that controllers should not take the impact estimation from previous data protection impact assessments as they are, without considering the context. The *Unguided Survey* assessed whether security and privacy experts distinguish privacy risks from security risks. The results showed that they confuse them, which may lead to non-compliance.

Chapter 4

Background

In this chapter we introduce some concepts and the two tools that we have employed to build our methodology. Section 4.1 introduces the GDPR, and Section 4.2 introduces the DPIA which we aim to assist controllers to conduct. Then we introduce privacy goals (see Section 4.3)—that we need to meet to comply with the DPIA—and privacy strategies (see Section 4.4)—that are used to implement privacy goals. Section 4.5 introduces RiskML tool that we have adapted for risk modeling and evaluation; the tool allows to address the P_{risk} (see Section 2.3.1) by enabling controllers to perform what-if analysis. Section 4.6 introduces another adapted tool that we have employed to check for compliance of user-specified access control policy, as under the GDPR it is not only enough to enforce access control policy but they need to be in alignment with the Regulation. For example, while not granting access to data subjects is not considered to be a risk from the classical risk analysis perspective, under the GDPR it is infringing data subjects' right and thus consider to be a risk.

4.1 General Data Protection Regulation

General Data Protection Regulation (GDPR) aims to strengthen and harmonize data protection regarding the processing of personal data. It requires consistent and high-level protection of the natural person, removes obstacles to flowing personal data within the European Union, and addresses the export of personal data outside the EU to protect personal data of individuals residing in the Union regardless of location. Following are some definitions which we will use throughout this document:

- "*Data subject*" refers to an identified or identifiable natural person;

- "*Personal data*" denotes any information that directly or indirectly allows identifying the data subject, in particular by reference to information to an identifier such as name, identification number, location data, or to one or more factors specific to the physical, physiological, genetic, mental economics, culture or social identity of that natural person;
- "*Special category of Personal data*" is a category of personal data which reveals: religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data to uniquely identify a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation;
- "*Data processing*" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- "*Controller*" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
- "*Data processor*" means a natural or legal person, public authority, agency or other body which processes personal data—by following documented instruction by data controller—on behalf of the controller.; unless required to do so by Union or Member State law to which processor subjects to;
- "*Recipient*" is a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not;
- "*Supervisory authority*" is one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons concerning processing and to facilitate the free flow of personal data within the Union (Article 51.1).

The GDPR allows data processing only if the data controller and data processor are able to comply with the Regulation. They shall: a) take appropriate measures to protect data against unlawful processing, b) provide relative information to data

subjects and supervisor authority, c) to exercise data subject right upon request, without undue delay.

The GDPR emphasizes on identifying and evaluating risks to data subjects' rights and freedoms, and accordingly to introduces countermeasures to prevent or reduce their impact on data subjects. For instance, recital 83 states that "to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption"; and article 24 states that "taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation [...]".

The GDPR is the first regulation that mandates controllers to conduct a Data Protection Impact Assessment (DPIA). Privacy Impact Assessment has been around since the 1990 [VDGR16]. However, it has not been an obligation until the GDPR came to enforcement. The introduction of DPIA in the Regulation can be seen as part of a broader risk-based turn in the field of data protection regulation and legislation [VZ16]. The Article 29 Working Party (replaced by the European Data Protection Board (EDPB)) states that the DPIA is a process for building and demonstrating accountability)[Arta].

4.2 Data Protection Impact Assessment

Article 35 of the GDPR introduces the Data Privacy Impact Assessment (DPIA). Controllers are responsible to conduct a DPIA to demonstrate compliance with the GDPR. Although the DPIA has no direct historical lineage, it has similarities with the Privacy Impact Assessment [VDGR16]. The DPIA is considered to be a risk-based approach to data protection. Recital 90 of the GDPR outlines some components of the DPIA that overlap with risk management steps (e.g., ISO 3100026). the DPIA under the GDPR is a tool for managing risks to the rights of the data subjects, and thus takes their perspective, that is, unlike risk management in other fields (e.g. information security) which are focused on the organization [Arta].

The controller shall carry out the DPIA and implement appropriate measures based on the output of the assessment. DPIA is required whenever the processing is likely to result in a high risk to the rights and freedom of natural person; in particular when the processing:

- requires new technology;
- is based on automated processing, including profiling¹;
- requires large scale special category of personal data or data related to criminal convictions and offense;
- requires systematic monitoring of large-scale data which is publicly available.

Article 35.7 states that the assessment shall contain at least:

- a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned

There is no further elaboration on when to conduct a DPIA and how to perform the steps mentioned above.

To assist controllers to carry out the assessment, the EDPB [Arta] proposed an iterative seven-step process, illustrated by Figure 4.1. The EDPB also does not provide further description on their proposed steps.

The main purpose of this thesis was to assist controllers in the process of conducting a DPIA. Therefore, we proposed an assisted iterative methodology that comprises three steps: *Processing Analysis*, *Risk Analysis* and *Run-time Analysis*. The steps of our methodology covers the seven steps process proposed by [Arta], and illustrated in Figure 4.1. Our first step covers their first two steps, our second step covers step three to five, and our last step covers their last step. Each step of our methodology outputs a document, which covers the sixth step of the process proposed by [Arta].

¹"Profiling" means any form of automated processing of personal data consisting the use of personal data to evaluate certain personal aspect of an individual, in particular to analyze and predict aspects concerning that natural person's performance at work, economic situation, personal preferences, interest, reliability, behavior, location, or movements.

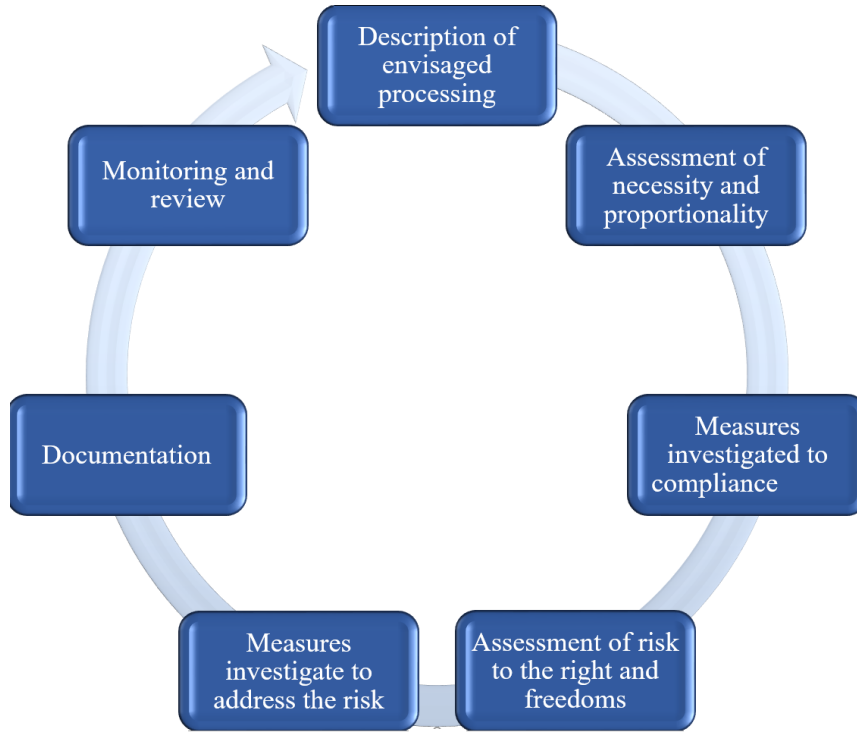


Figure 4.1: The DPIA Process, Proposed by [Arta].

4.3 Privacy Goals

As security goals (confidentiality, integrity, and availability (CIA)) categorize capabilities and controls of the system to achieve security outcome, so does privacy goals [BGL⁺17]. Recent research efforts have come up with privacy goals [RP09, Han11, DDFH⁺15, RB11], to provide an interdisciplinary standard model to assess and judge the consequences of utilizing complex IT systems concerning privacy and data protection [HJR15]. The privacy goals are: *CIA, unlinkability, transparency, and intervenability*. Information security is concerned about the unauthorized actions that lead to lose CIA of the information system, while privacy concerns both authorized and unauthorized actions [BGL⁺17]. Thus protecting the security goals also matters to preserve privacy. As the CIA are well-known, below we discuss only the last three privacy goals.

Unlinkability refers to hiding the link between two or more actions, identities, and pieces of information [DWS⁺11]. It relates to the principle of necessity and proportionality which consider *purpose determination and limitation, data minimization* [HJR15, DDFH⁺15], and *storage limitation*.

Purpose determination and separation require to collect personal data for specified, explicit and legitimate purposes and not be further processed in an incompatible manner with those purposes. Article 89(1) allows further processing for archiving purposes in the public interest, the scientific or historical research purposes or the statistical purposes.

Data minimization requires adequate, relevant and limited data to what is necessary for the purpose of the processing (article 5.1.c and article 35.7.b). *Storage limitation* requires keeping the personal data in a form that permits identification of data subjects for no longer than necessary for the purposes of data processing. Personal data may be stored for longer periods insofar as the personal data will be processed solely for achieving purposes in the public interest, scientific research or statistical purposes in accordance with Article 89(1), that is, subject to the implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (article 5.1.e).

Transparency, as requested by articles 5.1.a and 12.2, enables direct control by entitled entities, such as the data processing organization itself, a supervisory authority, or the affected human individual whose personal data is processed [HJR15]. Transparency is a prerequisite for *accountability* that is requested in article 5.1.

Intervenability requires the controller to facilitate the exercise of data subject rights under Articles 15 to 22, such as rights to access, rectification or erasure of personal data, and restriction of processing concerning the data subject. Data subjects rights are articulated from Articles 15 to 21,

4.4 Privacy Strategies

A strategy describes a fundamental approach to achieve a certain goal. Hoepman [Hoe14] introduces eight privacy design strategies derived from existing privacy principles and data protection laws, thus bridging the gap between the legal and the technical domain. They aimed to provide an accessible model in which system engineers can consider privacy protection during the analysis and requirements engineering phase [CHH16]. The strategies are the followings:

1. Minimise: Limit as much as possible the processing of personal data;
2. Separate: Separate the processing of personal data as much as possible;
3. Abstract: Limit as much as possible the detail in which personal data is processed;

Table 4.1: Eights Privacy Strategies and their Tactics.

Strategy	Minimize	Hide	Separate	Abstract
Tactics	Exclude Select Strip Destroy	Restrict Mix Obfuscate Dissociate	Distribute Isolate	Summarize Group
Strategy	Inform	Control	Enforce	Demonstrate
Tactics	Supply Notifies Explain	Consent Choose Update Retract	Create Maintain Uphold	Audit Log Report

4. Hide: Protect personal data, or make it unlinkable or unobservable. Make sure it does not become public or known;
5. Inform: Inform data subjects about the processing of their personal data in a timely and adequate manner.
6. Control: Provide data subjects adequate control over the processing of their personal data.
7. Enforce: Commit to processing personal data in a privacy-friendly way, and adequately enforce this.
8. Demonstrate: Demonstrate you are processing personal data in a privacy-friendly way.

To make the strategies more concrete, authors in [CHH16] refined the strategies by defining tactics that provide ways in which the overarching strategy can be made more concrete. Table 4.1 lists the tactics introduced for each strategy. Following the work in [Ahm20] and [Riv19], we have used the privacy strategies and their tactics to meet privacy goals. We elaborate on that in Chapter 2.

4.5 RiskML Tool

In [SMS14, FKM⁺15] authors introduced a tool-supported framework for risk modeling and evaluation, called *RiskML*². The framework is supported by a modeling language and a quantitative reasoning algorithm to analyze models. The RiskML tool considers an offensive analysis that is not provided by other available state-of-the-art tools, such as [LSS10]. It provides a conceptual formalism that provides a

²Please find the tool in <https://github.com/RISCOSS/riscoss-risk-modeling>

simplified risk assessment procedure by providing: (i) a good representation of the application domain under analysis; (ii) a proper representation of the goals of the implementer; (iii) provides a way to assess how the risk can propagate on goal; and (iv) provides the possibility to perform what-if analysis.

In order to provide the conceptual formalism, the RiskML language relies on the following components:

- a *situation* illustrates the circumstances under which a certain risk holds;
- an *indicator* is an abstract representation to determine the evidence of being in a certain situation. The value of an indicator by definition ranges between 0 and 1, where 0 means there is no evidence that the situation holds and 1 means there is evidence;
- an *event* illustrates the situation that has a negative impact on goals;
- a *goal* illustrates what the stakeholder aims to protect;
- a *risk* is defined as a tuple $\langle S, E, G \rangle$ where: S are the situations in which risk events potentially occur, E is the event whose occurrence impacts on stakeholder goals, and G is the goal which suffers a negative impact if the event occurs.

These components connect to one another with relations, as follows:

- *expose* from a situation to an event: the higher the evidence that the situation is satisfied, the more likely the event is to happen;
- *protect* from a situation to an event: the higher the evidence that the situation is satisfied, the less likely the event is to happen;
- *impact* from an event to a goal: the more the event is likely and the more its consequences are severe, the more the goal is at risk to fail; and
- *indicate* from an indicator to a situation to indicate whether the situation is satisfied.

All relations can be weighted to determine the significance of their effect. The weight on the relation *expose* indicates the likelihood of the event to happen; on relation *protect* indicates how the likelihood decreases if the corresponding situation holds; and on *impact* defines the *impact* level that the event could have on the goal. The tool calculate the risk level of the goal by multiplying the likelihood

level/protection level by impact level. Figure 4.2.a represents a RiskML model. It shows that the *Situation 1* and *Situation 2* are satisfied (their indicators are set to 1), while the *Situation 3* is not. When there is more than one situation connected to an event—either with *expose* or *protect* relation—the weight that the event gets is the maximum among them. Thus the risk level of goal in the example is $(+15, -0)$, which is the risk level of the goal is $+15$ (likelihood times impact) and there is no treatment to decrease that.

The RiskML tool captures how an event propagates through the model. Figure 4.2.b represents that *event 2* can happen as *Situation 3* is satisfied. Moreover, *event 1* leads to *event 2*, which implies that if the former occur the latter will also occur. The likelihood level of *situation 3* is 1, while the the likelihood of *event 1* is 3. As such the likelihood of *event 2* will be the maximum. Thus, the risk level of *Goal 2* is 6.

The RiskML tool provide the possibility to perform what-if analysis. So that the controller can see how the risk level will change if s/he were to configure the system differently. As such, the controller can make informed decision, considering the trade-off between the level of protection to get and the investment. Implementing security countermeasures are costly. Figure 4.2.b represents preforming what-if analysis for the given example above. That is, what if the *Protect Situation* were satisfied? In that case, the risk level would be $(+15, -10)$, which means the treatment can decrease the risk exposure to -10 .

To calculate the risk level, one approach could be taking the maximum value among the situation which protect/expose the system (as the RiskML does). Another approach could be summing the values. The second approach fits better in the context of our analysis. We elaborate on that further in Section 5.3.6.

We have adopted the RiskML tool to automatically generate the risk model from the collected information concerning employed and overlooked security and privacy controls, their vulnerabilities and vulnerabilities of supporting assets (see Section 5.3.6). As the tool allows to perform what-if analysis, controller can see how the risk level changes if data processing has been done with different configurations and so how to minimize the risk—that is to address P_{risk} .

4.6 Automated Access Control Compliance Checking

The literature on the security analysis of access control policies offer a wide range of techniques to automatically solve several policy analysis problems (see, e.g.,

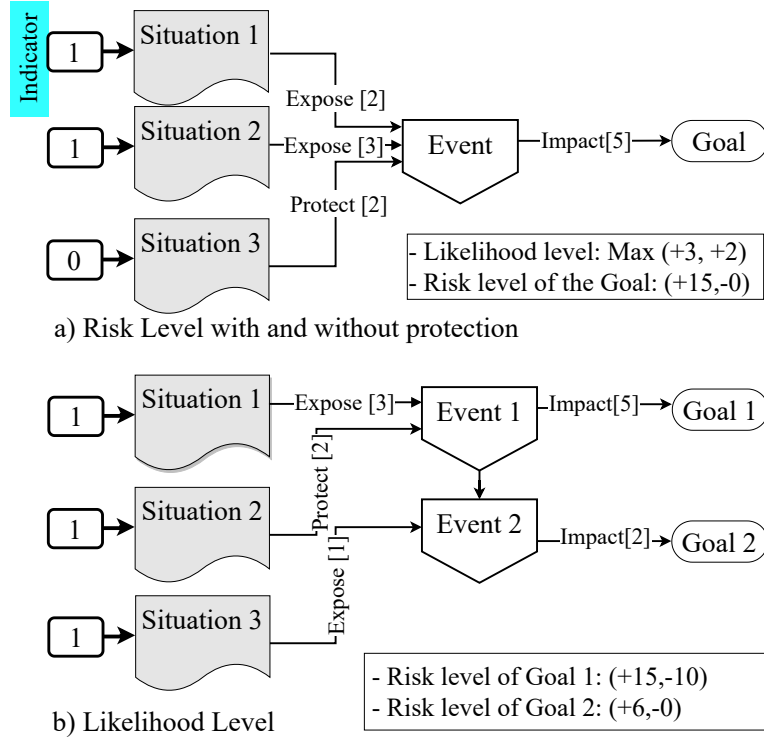


Figure 4.2: An Example of RiskML Model.

[TdHRZ17]). One of such problems is that of refinement; a policy p refines a policy p' iff every authorization request permitted or negated by p is also so by p' . The tool proposed in [GRS17, RS17] reduces the compliance of the access control policy p of the organization with respect to the European Data Protection Directive (EU DPD)—that is replaced by the GDPR—to check that p refines the policy obtained by instantiating a selected subset of the articles of the directive that are relevant to access control and to the data processing activity. In this way, every authorization request permitted or negated by the organization's policy is also so by the policy derived from the directive. The automated legal compliance checking tool proposed in [GRS17, RS17] checks the compliance of data processing with three main ingredients: (i) a formalization of the EU DPD, (ii) a mean to instantiate it to the information system under consideration, and (iii) techniques to check compliance.

For (i), legal and IT security experts collaborated to identify the parts of EU DPD that relate to purpose-aware access control policies. They have discarded provisions (a) from which it was impossible to derive access control rules and (b) those requiring substantial human interpretation. To do that, they have defined the following four auxiliary notions: (1) Purpose (Pur), (2) Consent (Cons), (3) Data Quality (DQ), and (4) Member State Requirement (MSReq). An example of MSReq is the

following: “Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing [...] by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing [...]” (article 6.2). They also identified two main relationships between controller (DC) and data subjects (DS) or processor (DP), which are *Mandate* (Man) and *Empower* (Emp). The former captures the delegation of operation to the processor by the controller, and the latter captures the operations that data subjects are empowered to execute. To derive the formal rules of the template access control policies, they replaced the natural language text with auxiliary notions.

$$\begin{aligned} & DC \wedge Proc \wedge PD \wedge Pur \wedge Cons \vee \\ & DP \wedge Man \wedge Proc \wedge PD \wedge Pur \wedge Cons \end{aligned} \quad (4.1)$$

where $\vee$ is disjunction and $\wedge$ is conjunction. The expression 4.1 can be read as a controller (or a processor mandated by the controller) can process (Proc) Personal Data (PD) for an allowed purpose (Pur) with data subjects’ consent (Cons).

For (ii), they introduce *bridge structure* that aims to specify how the template policy should be instantiated to the system under consideration. For example, if the processing in question indicates that the controller give (r)ead and (w)rite (a)ccess to data subject for a given document. Its *bridge structure* would be:

$$\begin{aligned} & DC \wedge a = r \wedge document \wedge DS \vee \\ & DC \wedge a = w \wedge document \wedge DS \end{aligned} \quad (4.2)$$

To apply the methodology, first controller needs to draw the Message Sequence Chart (MSC) related to the system in consideration. MSC is a possible way to describe the plan to achieve the system goal. Then, s/he identifies the concrete access control policies for the roles involved to achieve the goal already captured by the MSC. Accordingly, s/he defines the bridge structure. Then s/he can use the third ingredient (iii), that is the automated tool for security analysis and compliance checking. The tool answers questions about the system design that are:

- *Do the concrete access control policy enable the execution of the scenarios described by the MSCs in the design?*
- *Do the concrete access control policy enable the execution of the scenarios described by the MSCs in the design?*
- *Is the concrete access control policy compliant with the (formalization of the) regulation?*

```

1 {
2   "rule": [
3     {
4       "label": ["art.6(1) (a)"],
5       "effect": "allow",
6       "predicate": ["controller", "process", "personal_data",
7                     "legitimate_purpose", "data_quality", "consent",
8                     "ms_requirements"]
9     },
10    {
11      "label": ["art.6(1) (a)"]
12      "effect": "deny",
13      "sufficient": "not_legitimate_purpose",
14      "predicate": ["controller", "process", "personal_data",
15                   "not_legitimate_purpose"]
16    }
17  ]
18 }

```

Figure 4.3: An Excerpt of Formalization of GDPR.

The IT system expert can use the results returned by the tool to revise the system design or the bridge structure when security or compliance issues are detected.

To comply with the GDPR it is not only enough to define and enforce access control policies, they should comply with the requirements of the Regulation. For example, classically if a controller does not give access to data subject to delete or transfer data it will not be consider a risk; while under the GDPR they put the rights and freedoms of data subjects at risk. As such, we have adopted the presented tool to check whether the user-specific access control policies complies with the requirements of the GDPR. For that, we have adjusted the presented methodology to work for the GDPR, by formalizing the access control-related articles to a machine-readable format to be processed by the automated tool. Figure 4.3 shows an excerpt of such formalization. It refers to article 6.1.a which states that processing shall be lawful when “the data subject has given consent to the processing of his or her personal data for one or more specific purposes”. The first rule, shown in the figure 4.3, states that the controller is allowed to process personal data for a legitimate purpose and upon data subjects’ consent. The second rule states that not having a legitimate purpose is sufficient to deny processing.

Chapter 5

An assisted Methodology to Conduct a DPIA¹

A good (D)PIA must [WFR13]:

1. identify the information flow;
2. capture privacy risks and introduce safeguards to counteract;
3. review and update throughout the life of a project; and
4. provide a structure for the PIA report.

We propose an iterative assisted methodology to conduct a DPIA. It comprises of three steps: *Processing Analysis*, *Risk Analysis* and *Run-time Analysis*, depicted in Figure 5.1. Each step outputs a document, namely *Processing specification*, *Risk Summary*, and *Asset and event mapping*. The steps cover the first three requirements of a good DPIA mentioned above, respectively, and the documents cover the last one. In this thesis, we have focused on the first two steps and their application to identity management solutions, and we have left the third step for future work. This chapter details the proposed assisted methodology to conduct the DPIA.

Structure of the Chapter. Section 5.1 provides an overview of the methodology and introduces a running example. Section 5.2 and 5.3 detail the two steps of the methodology, namely *Processing Analysis* and *Risk Analysis*; and their application on the running example. Section 5.5 concludes the chapter.

¹The work is published in [DR20a, DR20b]

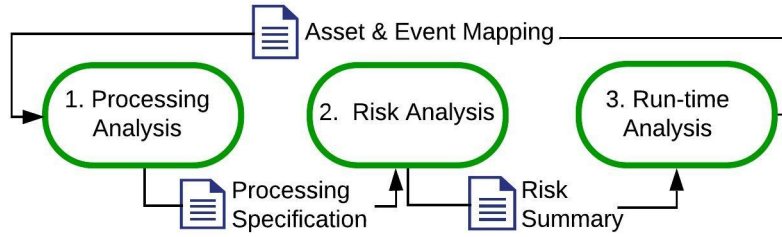


Figure 5.1: An overview of our methodology.

5.1 An Overview of the Methodology

The *Processing Analysis* step (Section 5.2) aims to acquire a comprehensive understanding of the organization, which is crucial to assess risks that the data processing may pose to the data subjects’ rights and freedoms and consequently to the organization. It assists the controller in identifying their required data type and data subject categories—as we learn they have difficulties doing so—to meet the principle of necessity and proportionality (article 35.7.b).

The *Risk Analysis* step (Section 5.3) aims to identify, evaluate and mitigate not only privacy risks but also security risks that could lead to infringing data subjects’ rights and freedoms. To do so, this step provides a hint for the controller to capture privacy threats—as they are not easy to identify—assess implemented security controls and privacy tactics and automatically assess whether the supporting assets and security/privacy technologies are vulnerable. Then, it automatically models the system as-is and provides the possibility of performing what-if analysis—using the adopted RiskML tool.

The *Run-time Analysis* aims to combine data analytic techniques with selected monitoring tools—such as those for Inventory Management (IM) and Security Information and Event Management (SIEM) to make our methodology continuous. The DPIA is “living” document [WFR13], it should be continuously reviewed and regularly reassessed [Arta].

It is difficult to establish a consensus on what needs to be reported in a (D)PIA report [ZWdH12, SO14]. In [SO14], authors have listed the elements that a PIA report needs to contain for different audiences. The list has four main categories: *general system information*, *assessment information*, *(D)PIA quality signals*, and *accountability*. The documents that our tool generates, cover the four mentioned categories as following: document *Processing specification* contains *general system information* and *PIA quality signals*; document *Security/Privacy Risk summary* contains *assessment information*; and document *Asset and event mapping* contains *accountability* information. These documents are a way to demonstrate compliance and to record

processing activities, as required by article 5.2 and 30, respectively. They are also helpful when communicating with stakeholders [Paj14].

A DPIA shall be conducted, prior to data processing, when the data processing is likely to result in a high risk to the rights and freedoms of natural persons. We do not provide any pre-assessment to check whether conducting a DPIA is necessary. For the following reasons:

- The minimum requirements that a DPIA shall contain, articulated in article 35.7, has already been asked in different articles of the GDPR:
 - article 12 requires a written description of the processing operation, as requested by article 35.7.a;
 - article 5 requires purpose limitations and data minimization, as requested by article 35.7.b; and
 - article 32 requires to assess risks to rights and freedoms of data subjects, as requested by article 35.7.c, d.
- Article 35.3 lists the conditions when risk is high. However, it is not an indicative/non-exhaustive list [Dem19]. For example, one condition is when a large scale of personal data is involved. Although [Boa] provides some indication on definition of *large scale*, yet it is not sufficient.² Indeed, recital 84 states that once a DPIA is conducted, one can indicate whether the processing involves a high risk.
- The EDPB [Arta] states that where it is not clear whether a DPIA is required, a DPIA is carried out nonetheless as a DPIA is a helpful tool to help controllers comply with data protection law.
- The office of the Australian Information Commissioner stated that the first question to ask about whether a (D)PIA is needed is “Will any personal information be collected, stored, used or disclosed in the project?” If the answer yes, then a (D)PIA is probably necessary [oAIC14]. Authors in [VvdB17] also believe that considering when conducting a DPIA is required, it might be necessary for most cases [VvdB17];

Yet, in the first step, the tool lists the conditions stated in article 35, under which conducting a DPIA is necessary. If one condition holds, the controller will be informed that conducting the DPIA for data processing in question is mandatory. Although, we encourage the controller to perform a comprehensive DPIA, anyways.

²<https://iapp.org/news/a/on-large-scale-data-processing-and-gdpr-compliance/>

There is a distinction between a data controller and a data processor: the former is the natural or legal person who determines the purposes and the means of processing, while the latter is the natural or legal person who processes the data on behalf of the controller, following strict instructions [GB018]. Yet, the GDPR obliges processors to comply with many of the requirements which apply to controllers, e.g., implement appropriate technical and organizational measures to ensure the security of processing. For the sake of simplicity, we only refer to the controller as the responsible role to follow the steps of our methodology.

Note, in our methodology, we focus on the processing that involves an individual, not the ones that aggregate data of several individuals by using big data or machine learning techniques. Indeed, there is a lot of data processing that uses neither of them and yet privacy critical. Such as public administrations' process to deliver certificates, e-government processes, or financial transactions that are inherently centered around the personal data of a single individual. For such processing, we consider the necessary access control permissions. For example, this considers operations that aim to process considerable amounts of data at a regional, national or supranational level or when otherwise potentially affecting a large number of data subjects [VvdB17].

Figure 5.2 represents a detailed overview of the methodology. For each step, it represents the introduced components to automate the process of fulfilling the goal of the step, and their related inputs and outputs. It also indicates where the process is automated and when controllers' input is required. We have adopted two tools, namely *Automated Access Control Compliance Checking* and *RiskML* (introduced in Chapter 4), which are indicated with dash-border rectangles.

Running Example. To illustrate the main concepts of our methodology, we consider the following example, taken from [GRS17].

An Italian research organization, called ITOrg, needs to compute the salary slips of its employees. Employee shall fill in a form, named profile, with some information such as name, surname, address, number of kids, type of contract, etc. Employee shall sign the document and send it to ITOrg. Employee needs to give their consent to use this information to compute their salary slip. ITOrg delegates computing of the salary to its Financial Department (Fin Dept) to confirm the working hour and type of contract. The Fin Dept receives selected parts of the profile, in a document called fin_profile. In turn, Fin Dept sends it to a company called ACME to compute the salary. Once done, ACME sends the salary slip back to Fin Dept, in a document called Salary, and they forward it to Employee.

5.2 Step 1. Processing Analysis

5.2.1 Overview of the Step

The step focuses on assessing and collecting information (articulated in articles 13 and 14) on the context of data processing that the organization in question conducts. That is necessary for assessing risks and to communicate them with the data subjects. We do this in two sub-steps: (1) introducing organization, that is, to indicate the roles, purpose, and involved data type and the data subject; and (2) introducing data processing, that is, to indicate specification of each data processing carried by the organization, by identifying the involved data type, data subject, and possible privacy risks, etc., related to the data processing in question. The information in (1) shall be specified once for all, while (2) shall be repeated for every data processing that the controller conducts.

The output of this step is a document, called *Processing specification*. It represents the information related to the organization and data processing it conducts that need to be communicated with data subjects and supervisory authority on request (request in article 12, 13 and 30). Below, we explain these two sub-steps.

5.2.2 Introducing the Organization

This sub-step gets to know the organization as a whole, and needs to be done once for all. This step requires controllers to identify the roles and some information about them, data type and data subject categories. Our tool provides a form where the controller needs to fill out this information.

Identifying the Roles. As requested by article 13.1.a and b, the controller needs to identify the identity and the contact details of the controller and, where applicable of the controller’s representative and the data protection officer.

Identifying Data Type and Data Subject Categories. Our experience to carry DPIA for the public administration in Trento, Italy, taught us that controllers have difficulties identifying categories of data and data subjects required for their data processing. In some cases, they collect data categories that are not necessary for their purposes. This compromises the principle of necessity and proportionality (article 35.7.b), and data minimization principle (article 5.1.c). These principles require access to necessary personal data [Sup] and data subject categories [Hoe18, Sup]

to fulfill the purpose of processing. They are necessary and a foundation step to engineer systems in line with privacy principles by design [GTD11].

To assist controllers, we have associated the most likely categories of data type and data subject to each economic sector [DR20b]. The association is based on the ultimate purpose that each economic sector has. For example, the economic sector *pre-primary education* aims to educate students from the age 4 to 7. Thus, they need personal data of data subjects who, according to article 8.1, are considered to be children. That implies that the processing of data subjects in this sector requires consent collected from the holder of parental responsibility for the child. Accordingly, we associate data subject categories *minor* and *parents* (article 8.2), and data type category *personal data* to this economic sector. NIST Publication 800 – 60 uses a similar approach, that is, identifying mission-based information type categories of organization [NIS08].

We have taken the nested economic sectors from the Standard classification of Economic Activities in the European Community, called NACE (Nomenclature des Activités Économiques dans la Communauté Européenne).³ NACE identifies 21 nested economic sectors. For example, economic sector *Education* consists of *pre-primary education*, *secondary education*, *educational support activities*, etc.; where *secondary education* consists of *general secondary education* and *technical and vocational secondary education*.

To have a fine-grained association, we have identified data type and data subject categories. The data type categories are the following: Personal Data (PD), Special category of Personal Data (SPD) and Personal Data with High Risk (HR). While PD and SPD are taken from the GDPR (articles 4 and 9.1, respectively), we have introduced Personal Data with High Risk (HR), to make the classification more fine-grained. The data assigned to this category are more sensitive than personal data, in terms of the impact in case of a data breach, but less than the special category of personal data. HR comprises of the followings: identification number; location data; an online identifier or to one or more factors specific to the physical, physiological, mental, economic, cultural or social identity of that natural person; personal data relating to criminal convictions and offenses. They are taken from articles 87, 4.1, and 10. The data subject categories are the followings: *Employee*, *Minor*, *Citizen*, *Parent*, *Patient*, *Collaborator*, *Natural Person*, *Legal Person*, *Student*, *Nominee*, *Detainee*, *Police/Military forces*, *Disable*, *Professor/teacher/trainer*. Table 5.1 shows the association of data type and data subject categories to economic sectors. The colored cell represents the main sectors. The sub-sectors inherit data type and data subject categories from their main sector; sub-sectors are listed where they can access other data type or data subject categories than their main sector. For instance,

³https://ec.europa.eu/competition/mergers/cases/index/nace_all.html

Table 5.1: Data Type and Data Subject category related to Economic Sector

Economic Sector	Data Subject Category	Data Type category
A - Agriculture, forestry, and fishing	Employee, Collaborator	Personal data
B - Mining and quarrying	Employee, Collaborator	Personal Data
C - Manufacturing	Employee, Collaborator	Personal Data
D - Electricity, gas, steam, and air conditioning supply	Employee, Collaborator, Natural and Legal person	Personal Data
D35.1.3 - Distribution of electricity		Financial data (HR)
D35.2.2 - Distribution of gaseous fuels through mains		Financial data (HR)
E - Water supply; sewerage; waste management and remediation activities	Employee, Collaborator, Natural and Legal person	Personal Data
E36 - Water collection, treatment, and supply		Financial data (HR)
F - Construction	Employee, Collaborator	Personal Data
F41 - Construction of buildings	Natural person, Legal person	Personal Data
G - Wholesale and retail Trade; repair of motor vehicles and motorcycles	Employee, Collaborator, Natural and Legal person	Personal Data
H - Transporting and storage	Employee, Collaborator, Natural and Legal person	Personal Data Financial data (HR)
H49 - Land transport and transport via pipelines		Location
H50 - Water transport		Location
H51 - Air transport		Location
H52.2 - Support activities for transportation	Minor	Health data
I - Accommodation and food service activities	Employee, Collaborator	Personal Data
I55 - Accommodation	Natural person , Minor, Disables	location
J - Information and communication	Employee Collaborator	Personal Data
J61 - Telecommunications	Citizen, Legal person	location
K - Financial and insurance activities	Employee, Collaborator, Legal person, Natural person, Minor, Disable	Health data, Personal Data, Financial data (HR)
K65 - Insurance, reinsurance and pension funding, except compulsory social security	Minor, Disable	
L - Real estate activities	Employee, Collaborator, Natural and Legal person	Personal Data, Financial data (HR)
M - Professional, scientific, and technical activities	Employee, Collaborator, Natural and Legal person	Personal Data
M69 - Legal and accounting activities		Special category of Data Financial data (HR)
M72 - Scientific research and development	Professor, Student	Special category of Data
M74 - Other professional, scientific and technical activities	Professor, Student	

N - Administrative and support service activities	Employee, Collaborator, Natural and Legal person	Personal Data
N77 - Rental and leasing activities		Financial data (HR)
N77.1 - Renting and leasing of motor vehicles		
N77.2.1 - Renting and leasing of recreational and sports goods		
N77.3 - Renting and leasing of other machinery, equipment, and tangible goods		
N77.4 - Leasing of intellectual property and similar products, except copyrighted works		
N79 - Travel agency, tour operator and other reservation service and related activities	Minor	
N80 - Security and investigation activities	all	Special category of Data
N82.2 - Activities of call centers		Location
O - Public administration and defense; compulsory social security	Employee, Collaborator	Special category of Data
O84.1 - Administration of the State and the economic and social policy of the community	Employee, Collaborator	Special category of Data
O84.2.1 - Foreign affairs	Nominees	
O84.2.2 - Defense activities	Police/Military, Natural person	
O84.2.3 - Justice and judicial activities	Detainees, Natural and Legal person, Minor	
O84.2.4 - Public order and safety activities	Citizen, Natural person	
O84.2.5 - Fire service activities	Citizen, Natural person	
O84.3 - Compulsory social security activities	Citizen, Natural person	
P - Education	Employee, Collaborator, Professors, Student/Trainee	Personal Data
P85.1 - Pre-primary education	Minor, Parents	
P85.2 - Primary education		
P85.5 - Other education		
P85.5.1 - Sports and recreation education		Health data
P85.5.3 - Driving school activities	Student	
P85.6 - Educational support activities	Minor, Parents	
Q - Human health and social work activities	Employee, Collaborator, patient Minor	Personal Data, Health data
R - Arts, entertainment, and recreation	Employee, Collaborator, Citizen Natural person	Personal Data
R90 - Creative, arts and entertainment activities	Minor	
R91 - Libraries, archives, museums, and other cultural activities	Minor	

S - Other services activities	Employee, Collaborator, Natural person	Personal Data
S94.1.2 - Activities of professional membership organizations		Trade union membership
S94.2 - Activities of Trade unions		Trade union
S94.9.1 - Activities of Religious organizations		Religious opinion
S94.9.2 - Activities of political organizations		Political opinion
T - Activities of households as employers; undifferentiated goods - and services - producing activities of households for own use	Employee, Collaborator	Personal Data
U - Activities of extraterritorial organizations and bodies	Employee, Collaborator	Personal Data

Legal and accounting activity is a sub-sector of *Professional, scientific and technical activities* sector, which can access *SPD* and *financial data* from *HR* category (as allowed in article 9.2.f), as well as *PD*; and data subject categories: *Employee, Collaborator, Natural person, Legal person*.

Controllers need only to select the economic sector to which their organization belongs, and the tool provides a list of related categories of data and data subjects. This restricts their choices to fulfill data minimization, proportionality and necessity principles. However, the tool allows controllers to add other categories if needed and ask them to explain the need. Note that the controller identifies data type and data subject categories required for any data processing they conduct in this step. The next sub-step, where the controller defines the data processing, s/he identifies required data type and data subject categories for data processing in question. This process is fully transparent to the controller. We have used automated reasoning techniques to mechanize the suggestion generation activity. We encode the association of sectors to categories of data type and data subject into formulae of propositional logic and use the capabilities of a constraint solver to generate the hints.

Once the controller submits the form, the tool leads her/him to the next form. The selected data type and the data subject will be input to the next sub-step, namely *Introducing Data Processing*.

5.2.2.1 Application of the Step on the Running Example

ITOrg is the controller and no joint controller is defined. The contact details of the controller and data protection officer are provided.

The organization falls under the sub-sector *Scientific research and development*. Thus, they are allowed to access data type *SPD* and *HR*—they are necessary for archiving purposes in the public interest, scientific or historical research purposes (article 9.2.j)—as well as *PD*. The following data subject categories are involved: *Employee, Collaborators, Natural and Legal person* as well as *Student, Professor, Patient* and *Disable*. Data are collected from data subjects involved.

5.2.3 Introducing Data Processing

The controller shall provide detailed information about the data processings they conduct. The previous sub-step has collected information about the organization in question as a whole, while from this point on, the steps are focused on each data processing conducted by the organization. The controller needs to indicate information including:

- involved roles;
- purpose of processing;
- data type categories involved and their source;
- supporting assets;
- duration of the process;
- impact level of data processing and the baseline; and
- information flow by means of Message Sequence Chart.

This sub-step provides controllers a form where they need to fill out the above-mentioned information.

Identifying the Involved Roles. The form asks the controller to identify whether the data processing involves a data processor(s). If any, the controller needs to indicate the name and contact details of the processor(s) and, where applicable, of the processor's representative. If any recipients, the controller needs to indicate the recipients or categories of recipients of the personal data (article 13 and 14).

Then, the involved data subject categories in the data processing in question needs to be identified. The controller has limited to the data subject categories indicated in the previous step.

Identifying the Purpose of Processing. To specify the purpose of processing, the tool provides two lists of legitimate purposes to access PD and SPD, derived from articles 6 and 9, respectively. The lists for PD contains the followings:

- data subject consented;
- required for the performance of a contract in the field of employment;
- required for compliance with a legal obligation to which the controller is subject;
- required for vital interest of data subject or of another natural person;
- required for public interest or in the exercise of official authority vested in the controller;
- required for legitimate interests pursued by the controller or by a third party.

And for SPD contains:

- data Subject consented;
- to carry out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law;
- required for vital interest of data subject or of another natural person;
- required for legitimate activities by a foundation, association or non-for-profit body with a political, philosophical, religious or trade union aim;
- manifestly made public by the data subject;
- exercise or defense of legal claims or whenever courts are acting;
- required for the public interest;
- it is for preventive or occupational medicine, for the assessment of the working capacity of the employee;
- medical diagnosis, provision of health or social care or treatment or management of health or social care systems and services;
- required for public interest in the area of public health;

- required for scientific or historical research or statistical purposes.

If the purpose is not on the lists, the controller can specify the purpose to justify the necessity of collecting the selected data type.

Identifying Data Type and Their Source. The controller needs to specify the data type involved in the data processing in question. As for data subject categories, the controller is limited to the chosen data type categories in the previous step. To indicate data types, the form asks first to name the document that represents the data. For instance, a document could be named *salary slip*, wherein from HD *financial data*, and from PD *full name*, *phone number* and *email address* are represented. This is following [Paj14] that distinguishes between data—that actors own, care about, and may deem confidential—and its representation via documents through which actors process data.

For each selected category of data, the controller asks to indicate the source from which the data is obtained, which could be either from data subjects themselves or other sources (article 14.2.f).

Identifying Supporting Assets. The tool asks the controller to specify the supporting assets used to process data in each stage of the processing that data are involved, which are when data are being collected *collection stage*, when being processed *processing stage*, and if when being sent to other involved roles (flow stage). For each identified supporting asset controller is asked, if possible, to specify the vendor name, product name, and the version of the product. If any, they will be reported in a JSON file called *NVDInput*. The file will be used to investigate if the employed technologies have any known vulnerabilities. We elaborate on this in Section 5.3.4.

Identifying Duration of the Process. The controller needs to estimate the duration of the data processing in question.

Estimating Impact Level and the Baseline. The controller needs to estimate the impact of data processing on data subjects' rights and freedoms. The impact evaluation is on a scale from 1 (negligible) to 5 (maximum). When (even) one of the following conditions hold, it indicates that data processing in question is likely to have a high impact on data subjects rights and freedoms:

1. usage of new technologies;

2. systematic and extensive evaluation of personal aspects relating to natural persons based on automated processing;
3. processing a large scale of special category of data;
4. processing a large scale of personal data relating to criminal convictions and offenses;
5. monitoring publicly accessible area on a large scale;
6. processing render it more difficult for data subjects to exercise their rights, or prevents it;
7. processing large scale of personal data that affects a large number of data subjects;
8. processing personal data of vulnerable data subjects, such as children, mentally ill persons, asylum seekers, or the elderly patients.

The conditions one to five are articulated in article 35.1 and 35.3, the sixth in recital 91; and the last two in [Arta].

In case that none of the above mentioned conditions hold, impact level will be automatically set as follows: *maximum* (scale 5) when special category of personal data, *significant* (scale 4) when personal data with high risks, and *moderate* (scale 3) when personal data are involved. Although the impact value is between 1 to 5, we do not assign lower than 3, as the GDPR requires adequate security even for (common) personal data. The estimated impact will be stored in a variable called *impactValue* and will input to the *Risk Analysis* Step (see Section 5.3).

Then, the baseline, discussed in Section 2.2.1, will be set according to the impact level of data processing. We consider the baseline be set as follows: *high* when the impact is *maximum* or *significant*; *moderate* when the impact is *moderate*, and *low* when the impact is *limited* or *negligible*. The identified information baseline for the data processing in question will be kept in a variable called *ProcessingBaseline*; and will be input in the Risk Analysis step.

Drawing Message Sequence Chart. Once the form is completed, our tool asks the controller to draw data flow of data processing in question by means of a Message Sequence Chart (MSC). Data flow identifies information flows, i.e., who collects which data, how the information is processed, who has access to it, with whom is the information shared, etc. [WFR13, Wri12]. It also helps to demonstrate the steps of a plan to achieve the declared purpose—that is an important aspect of privacy

protection to be able to specify and enforce purposes to assure data subjects that their data are processed as intended [DMGR15].

The tool drafts an MSC where the involved roles are added. The controller needs to identify the following information: (i) involved documents, (ii) privacy risks in each stage of data processing, and (iii) user-specific access control. We need these information for the *Risk Analysis* step (see Section 5.3). Below, we explain each of them.

(i) *Involved document*. The tool asks the controller to indicate the document involved in each stage of data processing. That shows how the personal data, represented by the document, flow.

(ii) *Privacy Risks*. Data processing may pose different risks to data subject's rights and freedoms. Controllers very often are not aware of or do not have the knowledge required to define privacy risks and so the privacy goals of a system [CG⁺16]. Indeed, we have learned that even information security and privacy experts confuse privacy risks with security risks (see Chapter 3). Hence, it is necessary to provide controllers with hints and suggestions, as also recommended in [CG⁺16]. As discussed in Section 2.2.2, we identify privacy risks through the privacy threats (*problematic data actions* introduced by NIST [NIS]). Each privacy threat could occur in different stages of data processing. Table 5.2 shows the stages where each privacy threat can occur.

In MSC, we consider that the *message exchange* tail indicates the source where the indicated documented is being collected from, that is *collection stage*; its point indicates where data are being processed, that is *processing stage*; and the *message exchange* itself indicates the flow, that is *flow stage*. While drawing the MSC, the controller is asked to capture relevant privacy threats. To do so, the MSC shows the related list of privacy threats assigned to each stage. For example, *distortion* can occur in *processing* and *flow* stage (see Table 5.2).

Once selected, the MSC adds the related privacy threats and their related goals and consecutive goals (see Table 2.1) to an array called *BadActionPrivacyGoals_Array*. This array later will be used to check whether any privacy tactics are implemented to counteract the identified threats (see Section 5.3.3).

(iii) *User-specific access control*. For each document the controller needs to indicate the granted access control to the sender and receiver. The granted accesses are: *read*, *write*, *update*, and *transfer*. We need to ensure that the access control policy complies with the requirements of the GDPR. Once the controller completes the MSC, it reports them in a file called *User-specified Access Control*. The file will be input to the *Automated Compliance of Access Control Policy* tool to be checked; that will be discussed in Section 5.3.5.

Table 5.2: Related Data Processing Stage of each privacy threat.

Stage	Privacy Threat
Processing, Flow	Distortion
Collection	Induced disclosure
Processing	Re-identification
Processing	Stigmatization
Processing	Surveillance
Processing	Surveillance
Processing	Appropriation
Collection, Processing, Flow	Insecurity
Processing, Flow	Unanticipated revelation
Processing	Re-identification
Processing	Appropriation
Processing	Unwarranted restriction

5.2.3.1 Application of the Step on the Running Example

Involved Roles. The controller specifies the following roles: fin Dept and ACME as processors, and employees as data subjects.

Purpose of Processing. The data processing in question is *computing salary slip*. The controller selects the following purpose from the list: *carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law*.

Identifying Data Type and Their Source. There are three documents involved in this processing:

- profile, which contains: *employees ID, full name, address, number of children, previous salary, work experience*;
- Fin_Profile, which contains: *employee ID, number of children, previous salary, work experience, type of contract and employee's work hour*;
- salary, which contains: *employee's ID and computed salary*.

The personal data represented by the document *profile* are collected from data subjects themselves, *type of contract* and *employee's work hour* are inserted automat-

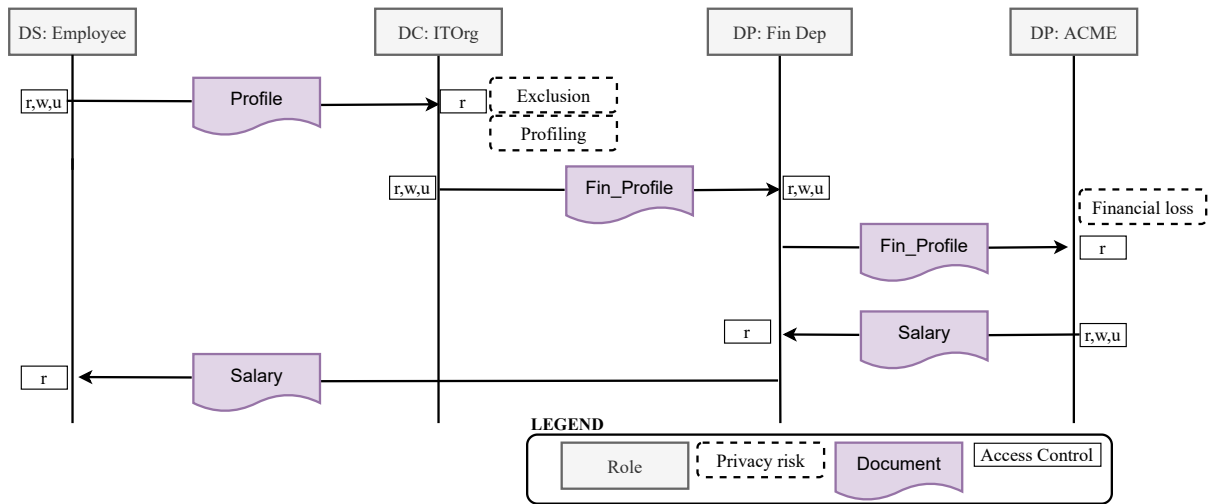


Figure 5.3: Annotated Message Sequence Chart of the Running Example.

ically by the system. While the other two documents are structured by ITOrg, and ACME, respectively.

Identifying Supporting Assets. The controller identified the following supporting assets: *HP Inkjet printer*, *ownCloud Server before 10.0.1*⁴, and *Sql server 2016*.

Identifying Duration of the Process. The data will be collected during each month (the working ours) and will be processed at the end of the month.

Estimating Impact Level and the Baseline. The impact of the processing is *maximum* As, according to [Arta], Employee is one of the vulnerable category of data subject. As such the variable *impactValue* will be set to 5; and *ProcessingBaseline* will be set to *high*.

Drawing MSC. Figure 5.3 illustrates the MSC of our running example. It shows that Employees have full access to their profile while controller can only read it. The controller and Fin_Dep have full access to document Fin_Profile, while they and data subjects can only read document salary, to which ACME have full access. The *User-specified Access Control* file will report them.

The controller from his side has chosen the privacy threat *appropriation* and *surveillance*. From the ACME side, he has chosen the privacy threat *distortion*.

As such *BadActionPrivacyGoals_Array* will be populated with the followings privacy threats: *appropriation*, *surveillance*, and *distortion*; and their related goals and con-

⁴ownCloud is a suite of client-server software for creating and using file hosting services; it has similarities to the widely used Dropbox.

secutive goals, that are: *purpose limitation*, *transparency*, *data unlinkability*, *purpose specification*, and *integrity*. (see Table 2.3).

5.3 Step 2. Risk Analysis

5.3.1 Overview of the Step

Current best practices on (D)PIA [Cla09, SWB⁺12, OSG⁺11, Artc, CNI12a] all agree that risk analysis is the key to conduct a (D)PIA. DPIA protects data subject's rights and freedoms with regards to the processing of personal data. The GDPR respects fundamental rights, particularly private and family life and the protection of personal data.

Controllers shall respect data subjects' right to data protection (recital 78). To respect that, controllers are required to take appropriate technical and organizational measures, including the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services (article 32.1.a). Moreover, controller shall ensure that the data processing does not infringe on data subjects' rights and freedoms. Accordingly, we introduce the following two sub-steps: (1) *supporting data subject's right to data protection*, (2) *supporting data subject's right to privacy*. The first sub-step (see Section 5.3.2) ensures personal data protection by meeting security goals (CIA trail). While the second sub-step (see Section 5.3.3) ensures that data subjects' rights are preserved by meeting privacy goals. We have explained the privacy goals in Section 4.3.

A risk is a scenario that describes how risk sources might exploit supporting assets [CNI12a, CNI12b] and security countermeasures vulnerabilities leading to cause an incident on primary assets and impacts on privacy. For examples *fax-ready HP OfficeJet inkjet printers* come out of the box with a static buffer overflow vulnerability, which allows remote code execution (CVE-2018-5925⁵); and *Microsoft ADFS 4.0 Windows Server 2016* and previous versions (Active Directory Federation Services) suffer from SSRF vulnerability (CVE-2018-16794⁶). Accordingly, we introduce the third step, that is, (3) *investigate vulnerabilities* (see Section 5.3.4).

Controllers may define and enforce access control policies in their organizations, which is enough from a classical risk analysis perspective. However, it is not enough to ensure compliance with the GDPR. For example, the classical risk analysis does not see any risk if a controller uses data subject's personal data for any purpose

⁵<https://nvd.nist.gov/vuln/detail/CVE-2018-5925>

⁶<https://www.cvedetails.com/cve/CVE-2018-16794/>

than the primary purpose for which data are collected, or if they do not give access to data subject to delete or transfer data. However, under the GDPR they put data subject privacy at risk. We observe that modern approaches decompose access control in three main components: policy language, model, and enforcement—see, e.g., [DFJS07]. The first two define in abstract mathematical terms the syntax and semantics, respectively, of access control policies, whereas the third specifies the mechanisms put in place to enforce the policies. One of the main advantages of this approach is to separate the analysis of high-level security properties from the correctness of the enforcement mechanisms. In fact, it is well-known that writing and maintaining policies is an error-prone activity because of the possibility of inserting redundancies, conflicts, and other logical problems—see, again [DFJS07] for an introduction to this and related problems. Similarly, guaranteeing the compliance of access control policies expressed in mathematical terms against legal provisions is difficult, even disregarding the risks deriving from vulnerable implementations of the enforcement mechanisms. Logical errors in access control policies prevent compliance already at the design level and thus constitute an important source of risk to identify and eliminate. As such, we introduce a fourth step, that is, (4) *compliance of access control policies* (see Section 5.3.5), where we use the tool proposed by [GRS17, RS17], and introduced in Section 4.6.

Finally, we want to generate a risk model where controllers can observe the risks that the system as-is may suffer from the risk level of each privacy and security goal. We also want them to observe how changes in the system configuration can change the risk level; so that they can take an informed decision on how to modify the system to reduce the risks to data subjects’ rights and freedom. That introduces the fifth step (5) *Modeling risk* (see Section 5.3.6), where we use the tool proposed by [SMS14, FKM⁺15], and introduced in Section 4.5.

Figure 5.2 indicates all the inputs and inputs of these sub-steps. The output of *Risk Analysis* step is a document called *Risk Summary*, that is created from the two documents: *Security Risk Summary*—generated in the first sub-step—and *Privacy Risk Summary*—generated in the second sub-step.

This step answers the two defined problems (see Section 2.3), namely P_{risk} and $P_{compliance}$. The former tackles security and privacy risk assessment and trade-off analysis; and the latter tackles compliance with security and privacy requirements of the DPIA.

Note that our methodology aims to assist controllers in conducting a DPIA by automating the process as possible—It is not to be replaced for a comprehensive privacy and security risk analysis.

t

5.3.2 Supporting Data Subject's Right to Data Protection

To protect data subjects' right to data protection, controllers require to take appropriate technical and organizational measures to ensure confidentiality, integrity and availability, and resilience of processing system and service (article 32.1.b).

To assist controller to provide a minimum security, we have built a *Security Reference Model* (see Section 2.2.1). The reference model is stored in a database called, *ControlReferenceModel_DB*. If the control wishes to employ other set of controls, s/he can simply update the database. We assess rights to data protection in two sub-steps:

1. assessing the implemented controls—that assesses $\mathcal{AF}_{\text{securityControl}}$ to prepare the inputs to address problem P_{risk} ;
2. assessing their compliance with requirements of the DPIA—that is to address security compliance part of $P_{\text{compliance}}$, that is, $\text{DPIA}_{\text{security}}$.

5.3.2.1 Assessing the Implemented Controls

To assess the appropriateness of implemented security control for the data processing in question, we use a questionnaire called *Control Questionnaire*. The questionnaire has three sections, one for each security goal (confidentiality, integrity and availability). For example, it asks:

- Do you prevent unauthorized information transfer via shared system resources?
- Do you validate user input?
- Do you have protection necessary for power equipment and cabling employed?
- Do you employ least privilege?

The above-mentioned questions relate to confidentiality; integrity; availability; and confidentiality and integrity, respectively. The controller's response could be: "Yes", "Partially implemented", "No", and "Not applicable". Whenever the answer is one of the first two, the controller is asked, where possible, to specify the implemented technology by specifying vendor, product and version. We use this information to investigate if the employed technologies have any known vulnerabilities. We elaborate on this in Section 5.3.4.

To generate the questionnaire, we use a generator called *Control Questionnaire Generator*. The generator takes the *Security Reference Model* (see Table 2.1) from *ControlReferenceModel_DB* based on which it generates the questionnaire.

The generator compiles the answers and calculates the likelihood and protection level. The levels (as for impact) are on a scale from 1 (negligible) to 5 (maximum). We assume that all the controls contribute equally to protect the system. However, if the answer is 'Partially implemented', the contribution of given control is half. To calculate the protection level, the generator considers how many security controls—from the applicable ones—are implemented. For example, if the controller has implemented 40 security controls out of 50 applicable ones, then the protection level will be 4 and likelihood will be 1. While if 10 out of 40 implemented controls are partially implemented, the protection will be 2. To calculate the likelihood, it subtracts the protection level from 5.

If any security technologies are specified by which the control is implemented, the generator updates the *NVDInput* documents.

Finally, the generator outputs a document called *Security Risk Summary* that contains: implemented security controls, and where indicated the employed security technology, overlooked security controls, and estimated likelihoods.

5.3.2.2 Assessing Compliance of Implemented Controls with the $DPIA_{security}$

The document *Security Risk Summary* will be input into a component called *Security BCP Checker*. The checker checks whether *applicable* security controls related to the data processing information baseline are implemented. The information baseline has already been estimated in the previous step (Section 5.2.3 where involved data types are specified) and stored in *ProcessingBaseline*. If the required controls are not implemented, the generator raises a warning and lists the overlooked controls.

5.3.2.3 Application of the Step on the Running Example

Assessing the Implemented Controls. The generator generates appropriate *Control Questionnaire* for a data processing with baseline *high* (since the related baseline to data processing in question is *high*). The controller responds to the questionnaire. The generator compiles the responses and report them in the document *Security Risk Summary*. Figure 5.4 illustrates a part of the generated output. The full version can be found in C.1. Following is the status of security controls, as generator reported:

```

1  {
2    "Confidentiality":
3    [
4      {
5        "SecurityControl": "Identification and authentication" ,
6        "Identifier": "IA-2",
7        "baseline": [{ "Low": ["IA-2"] },
8                      { "Moderate": ["IA-2"] },
9                      { "High": ["IA-2", "IA-3", "IA-4", "IA-8"] } ],
10       "question": "Do you provide any Identification and authentication?",
11       "Answer": "Yes",
12       "SecurityTechVendor": "Auth0",
13       "SecurityTechProduct": "Auth0.js",
14       "SecurityTechVersion": "8.10.1",
15       "OtherGoal": ["Integrity"]
16     ],
17     {
234    "Integrity":
235    [ { "SecurityControl": "Information handling and retention",
286      "Availability":
287      [ { "SecurityControl": "Information system backup",
334        "Likelihood":
335        { "Confidentiality":
336          { "total": "50",
337            "Applicable": "23",
338            "Implemented": "20",
339            "NotImplemented": "3",
340            "LikelihoodLevel": "0.7"
341            "ProtectionLevel": "4.3"
342          },
343          "Integrity":
344          {
352          "Availability":
353          {
362          }
363        ]
364      }
365    ]
366  }

```

Figure 5.4: An Excerpt of Control Questionnaire Output in JSON Format.

- Confidentiality

- Number of provided security controls: "50",
- Number of Applicable ones: "23",
- Number of Implemented ones: "20",
- Likelihood Level: "0.7"
- Protection Level: "4.3"

- Integrity

- Number of provided security controls: "42",

- Number of Applicable ones: "30",
- Number of Implemented ones: "21",
- Number of Not Implemented ones: "9",
- Likelihood Level: "1.5"
- Protection Level: "3.5"
- Availability
 - Number of provided security controls: "23",
 - Number of Applicable ones: "6",
 - Number of Implemented ones: "4",
 - Number of Not Implemented ones: "2",
 - Likelihood Level: "1.7"
 - Protection Level: "3.3"

The controller has defined the following security technologies, by which the document *NVD Input* will be updated:

- Vendor: "Auth0", Product: "Auth0.js", Version: "8.10.1";
- Vendor: "Microsoft", Product: "Active Directory Federation Services", Version: "4.0";
- Vendor: "Cisco", Product: "firepower management center", Version: "6.4.0";
- Vendor: "Juniper Networks", Product: "Junos Space", Version: "15.2";
- Vendor: "PulseSecure", Product: "Pulse Connect Secure", Version: "43";
- Vendor: "Microsoft", Product: "Azure Security center", Version: "".

Assessing Compliance of Implemented Controls with the DPIA_{security}. The *Security BCP Checker* checks whether the required security controls of the baseline are met. The checker warns that the following applicable security controls related to the information baseline are not implemented: *IA-3, AC-4, AC-19, SI-2, SI-4, SI-5, SI-10, SI-11, SI16, and CP-10*.

5.3.3 Supporting Data Subject’s Right to Privacy

To support data subjects’ rights to privacy, the controller needs to respect the rights articulated in articles 15 to 22, data processing principles articulated in article 5, and address any threats to data subjects’ rights and freedoms. We discussed, in Section 2.2.2, that by meeting privacy goals we ensure that we protect data subjects’ right to privacy. To address privacy goals, we have introduced the *Privacy Reference Model*. The model is stored in a database called, *StrategiesReferenceModel_DB*. If the control wishes to use other privacy tactics, s/he can simply update the database.

We assess data subject’s right to privacy in two sub-steps:

1. assessing the implemented privacy tactics—where we assess $\mathcal{AF}_{\text{PrivacyTactic}}$ to prepare the inputs to address Problem P_{risk} ;
2. assessing compliance with requirements of DPIA—that is to address privacy compliance part of $P_{\text{compliance}}$, that is, $\text{DPIA}_{\text{privacy}}$.

5.3.3.1 Assessing the Implemented Privacy Tactics

To assess the implemented privacy tactics for the data processing in question, we use a questionnaire, called *Right Questionnaire*, that asks the controller whether privacy tactics are implemented. For example, the questionnaire asks:

- Do you offer user basic functionality to have real choices over their personal data?
- Do you ask users explicit consent to the processing of their personal data?
- Do you notify users the moment you process their personal data?
- Do you prevent understandability of personal data?

The privacy goals mapped to the questions above are intervenability, purpose specification and intervenability, transparency, and data unlinkability, respectively. As for *Control Questionnaire*, the controller’s response could be: “Yes”, “Partially implemented”, “No”, and “Not applicable”. Whenever the answer is one of the first two, the controller is asked to specify, where possible, the employed technology by identifying *vendor*, *product* and *version*. If any, the generator updates the *NVDInput* documents. We use this information to investigate if the employed technologies have any known vulnerabilities. We elaborate on this in Section 5.3.4.

To generate the *Right Questionnaire*, we use a generator called *Right Questionnaire Generator*. The generator takes the *Privacy Reference Model* from *StrategiesReferenceModel_DB* to generate the questionnaire. Note that, the questionnaire does not question about privacy tactics related to *confidentiality* and *integrity*, as they are already addressed by *Control Questionnaire*.

The generator compiles the responses, and checks whether captured privacy risks by the MSC are addressed. If not, it raises a warning and lists the related privacy risks and overlooked strategies. For that, the generator gets the *BadActionPrivacyGoals_Array* (see Section 5.2.3) that lists the identified privacy threats and checks whether their related privacy goals are addressed.

It calculates the likelihood and protection level of each privacy goal, the same way as *Control Questionnaire Generator*.

The generator outputs a document, called *Privacy Risk Summary* that contains: implemented privacy strategies, and where possible the employed (privacy enhancing) technologies (PET); overlooked privacy strategies; and estimated likelihoods.

We propose a model that captures technologies, design solutions, and practical advice to meet the privacy tactics. The model assists the controller to choose the technologies that fit the requirements of their system. We have extracted them from [Ahm20, Riv19], which have a similar approach, that is, mapping the controls to tactics. Table 5.3 shows of the associations. For example, one privacy tactic to address privacy goal *data unlinkability* is privacy tactic *Mix*, that relates to privacy strategy *Hide*. [Ahm20] suggested PETs such as *Single proxies*, *VPNs*, *Tor service* to implement the tactic.

Other works such as [SO14, DWS⁺11, BEL17] have also introduced PET. Authors in [SO14] introduced seven categories of privacy target. We have matched them to privacy goals/privacy principles. Authors in [BEL17] have introduced measures to address data processing principles. Authors in [DWS⁺11] introduced them to address: Unlinkability; Anonymity/Pseudonymity; Plausible deniability; Undetectability/unobservability; Confidentiality; Content Awareness; Policy and consent compliance of the system. They related to *data unlinkability* and *confidentiality* (the first five), and *lawfulness*, *fairness* and *transparency*. We have listed their introduced measure in Appendix B.3.

5.3.3.2 Assessing Compliance with the DPIA_{privacy}

To ensure compliance, the controller needs to ensure that the data processing principles are met, data subjects' rights are preserved, and there are no privacy threats

Table 5.3: Mapping Privacy Goals to Privacy Enhanced Technology

Privacy Goal	Privacy Strategy	Tactic	Privacy Enhanced Technology	
			[Ahm20]	[Riv19]
Unlinkability: Data unlinkability	Hide	Mix	Single proxies, VPNs, Tor service, Mixmaster, Mixminion, Broadcast, Steganography, Watermarking, Anonymous remailer (awxcnx), Randomize browser fingerprints, ensure k-anonymity of sensor readings, Ensure spatiotemporal readings cover at least k individuals, Google Sharing, I2P, JonDo	mix-networks, multi party computation.
		Dissociate	Onion routing, RFID deactivation, Safe Harbor, Anonymouse, Hosts file domain blocking, Java anon proxy	privacy enhancing IAS, anonymous credential.
		Obfuscate	Single Proxies, VPNs, Differential privacy, (TrueCrypt) Steganography, Verifiable encryption, Lying, release noisy aggregates of data, obfuscate locations with planar Laplace noise, Apply noise to meter readings, Ensure correct usage of SSL/TLS with static analysis, Ensure correct usage of SSL/TLS with dynamically linked libraries, Secure public WiFi with WPA2, RetroShare	symmetric/public key, cryptographic libraries, verifiable encryption, secure elements, deniable encryption, oblivious transfer, steganography, spread spectrum, homomorphic encrypt, private preserve biometric, covert communication
	Separate	Distribute	Store private data only on private devices, Use secure distributed data storage	Private information retrieval
		Isolate	Implement Sensors only in specific places and inform data subjects, Smart meter, pay as you drive, Isolate sensors from other systems, Separate entities that ask for and receive sensor readings, Process data for smart metering on device, Process data for toll pricing on device, Hide access patterns to remote files, Hide access patterns to remote databases, Hosts file domain blocking, Privatix live-system	Private information retrieval
	Abstract	Summarize	K anonymity, Differential privacy, l-diversity, Query restriction, Sampling (Non-perturbative masking), Microaggregation, Release only data that satisfy k-anonymity, Ensure k-anonymity of sensor readings, Ensure spatio-temporal readings over at least k individuals, Use privacy-preserving data aggregation Aggregate data over multiple participants privately	k-anonymity, l-diversity
		Perturb		

Unlinkability: Data minimization	Minimize	Group	Top/bottom coding, Local suppression, Microaggregation, Reduce time and location granularity on device, Aggregate sensor readings from multiple participants privately, Aggregate data over multiple participants, Use privacy-preserving data aggregation,	k-anonymity, l-diversity	
		Exclude	Single proxies, VPNs, restrict cookies, disable cookies, Avoid use of third-party libraries, Do not store identifiers of smart cards, Reduce time and location granularity on device, Cluster IoT data streams and only release clusters with at least k members, Avoid storing encryption keys on device, Abine, Ad blockers, Anonymous, Internet proxy, Ixquick, MyTube	Private information retrieval, private preserve data mining, Differential privacy	
		Select	Extract relevant features on sensor, Cluster IoT data streams and only release clusters with at least k members	Searchable encryption	
		Strip	Statistical disclosure control, avoid storing encryption keys on device, Authenticate users without identifying them, Use short-lived pseudonyms for car-to-car communication, IRMA	Oblivious transfer	
		Destroy	discard raw data, Eliminate mapping between short-term and long-term identifiers, Ccleaner, Eraser	data removal tools	
	Abstract	Summarize	K anonymity, Differential privacy, l-diversity, Query restriction, Sampling (Non-perturbative masking), Micro aggregation, release only data that satisfy k-anonymity, Ensure k-anonymity of sensor readings, Ensure spatio-temporal readings over at least k individuals, Use privacy-reserving data aggregation, Aggregate data over multiple participants privately	k-anonymity, l-diversity	
		Perturb			
		Group	Top/bottom coding, Local suppression, Micro aggregation, reduce time and location granularity on device, Aggregate sensor readings from multiple participants privately, Aggregate data over multiple participants, Use privacy-preserving data aggregation,	k-anonymity, l-diversity	
	Unlinkability: Purpose specific	Inform	Supply	Privacy dashboard, RFID Logo, Privacy level agreements, Platform for privacy preferences (P3P), Privacy bird, Formal Framework: CI (Contextual Integrity), S4P, SIMPL, Pidder	Privacy icons, Feedback tool for privacy and awareness, Policy communication (P3P)

Unlinkability: Purpose limitation	Control	Explain	ToSDR, TOSBack, RFID Logo, Privacy level agreements (VisiOn Project), Privacy bird, PRIME,Panopticlick	Feedback tool for privacy and awareness
		Consent	Establishing PLA (organizational level), JITCTAs (Just-In-Time-Click- Through Agreements), Drag-and.Drop agreements (DADAs), Separate purposes (PLAs), Personalized negotiation, PrivacyFinder	
Transparency	Inform	Supply	Privacy dashboard, RFID Logo, Privacy level agreements, Platform for privacy preferences (P3P), Privacy bird, Formal Framework: CI (Contextual Integrity), S4P, SIMPL, Pidder	Policy communication(P3P)
		Notify	Lightbeam (Firefox), TaintDroid, Mobilitics, Data track, Certificate patrol, Electronic mail	
		Explain	ToSDR, TOSBack, RFID Logo, Privacy level agreements (VisiOn Project), Privacy bird, PRIME,Panopticlick	
Intervenability	Control	Consent	Establishing PLA (organizational level), JITCTAs (Just-In-Time-Click-Through Agreements), Drag-and.Drop agreements (DADAs), Separate purposes (PLAs), Personalized negotiation, PrivacyFinder	Feedback tool for privacy and awareness
		Choose	Compute statistics over sensor readings from participants privately, RABAC (for Buddy List), Selective access control, SPoC, c-Consent, TUKAN, Anonymous access, BugMeNot, TeamSpace, WebWasher	
		Update	Change device identifiers frequently to prevent fingerprinting, Data track, check-in model (broadcasting status), PLA (VisiOn Privacy Platform)	Feedback tool for privacy and awareness
		Retract	Reduce time and location granularity on device, cluster IoT data streams and only release clusters with at least k members, Implement levels of publicity, Anonymous access, BleachBit, Ccleaner	
Data Processing Principle				

Confidentiality	Hide	Restrict	Single proxies VPNs, Use cryptographically enforced role-based access control, Use identity-based encryption for private service discovery, Use attribute-based encryption for access control (RABAC), Authenticate users based on attributes instead of identities	context-based access control , privacy aware access control, policy enforce (XACML)
		Obfuscate	Single Proxies, VPNs, Retro Share (TrueCrypt)Steganography, Differential privacy, Verifiable encryption, Lying, release noisy aggregates of data, Obfuscate locations with planar Laplace noise, Apply noise to meter readings, Ensure correct usage of SSL/TLS with static analysis, Ensure correct usage of SSL/TLS with dynamically linked libraries, Secure public WiFi with WPA2,	symmetric/public key, cryptographic libraries, verifiable encryption, secure elements, deniable encryption, oblivious transfer, eganography, spread spectrum, homomorphic encrypt, private preserve iometric, covert communication
Lawfulness and fairness and transparency	Enforce	Create	Perform model-based PIA, Freenet, HTTPs everywhere	
		Maintain	PLA, KeePass	
		Uphold	Enforce honesty of device for local processing, enforce honesty of vehicle for local processing, Implement an orchestrator (a Javascript program as a App in client browser, the orchestrator makes sure that the identity broker can't correlate the original request from the service provider with the assertions that are returnedfrom the identity provider.), Sticky policies, EPAL	Feedback tool for privacy and awareness
Accountability	Demonstrate	log	Secure data logger strategy, Secure log store strategy, Stackdriver logging, MEMOIR, Autonomy CEN, Yenta	
		Audit	Java API for logging Log4J, Ghostery	
		Report	ClouDAT platform, VisiOn privacy platform, Ghostery	
Unlinkability: Storage limitation	Minimize	Destroy	discard raw data, Eliminate mapping between short-term and long-term identifiers, Ccleaner, Eraser	data removal tools
		Strip	Statistical disclosure control, avoid storing encryption keys on device, authenticate users without identifying them, Use short-lived pseudonyms for car-to-car communication, IRMA	data removal tools

against data subjects' rights and freedoms. As such, the controller needs to ensure that at least one tactic for each privacy goal is implemented, that is, all requirements mentioned above are met.

The document *Privacy Risk Summary* will be input into a component called *Privacy BCP Checker*. The checker checks whether at least one tactic per privacy goal is implemented. It raises a warning for any overlooked privacy goals.

```

1  {
2    "Data Unlinkability":
3    [
4      { "Tactic": "Mix",
5        "question": "Do you Mix personal data to hide the source or their interrelationships?",
6        "Answer": "No",
7        "SecurityTechVendor": "",
8        "SecurityTechProduct": "",
9        "SecurityTechVersion": "",
10       "OtherGoal": ""
11      },
12      { "Tactic": "Dissociate",
13      },
14      { "Tactic": "Obfuscate",
15      },
16      { "Tactic": "Restrict",
17      },
18      { "Tactic": "Isolate",
19      },
20      { "Tactic": "Distribute",
21      },
22      { "Tactic": "Summarise",
23      },
24      { "Tactic": "Group",
25      },
26      { "Tactic": "Perturb",
27      },
28    ],
29    "Minimization":
30    [
31      { "Tactic": "Select",
32      },
33    ],
34    "Transparency":
35    [
36      { "Tactic": "Supply",
37      },
38    ],
39    "Intervenability":
40    [
41      { "Tactic": "Consent",
42      },
43    ],
44    "Accountability":
45    [
46      { "Tactic": "Log",
47      },
48    ],
49    "Lawfulness":
50    [
51      { "Tactic": "Create",
52      },
53    ],
54    "Likelihood":
55    {
56      "Data Unlinkability":
57      {
58        "total": "8",
59        "Applicable": "6",
60        "Implemented": "2",
61        "NotImplemented": "4",
62        "Likelihood": "3.3",
63        "Protection": "1.7"
64      }
65    }
66  },

```

Figure 5.5: An Excerpt of Right Questionnaire Output in JSON Format.

5.3.3.3 Application of the Step on the Running Example

Assessing the Implemented Privacy Tactics The controller responded to the questionnaire. Figure 5.5 illustrates a part of the generated output. The full version can be found in Appendix C.2. The controller has not defined any implemented PETs.

The generator then checks whether any privacy strategies are in place to address the identified privacy risks. The *BadActionPrivacyGoals_Array* reports the following

privacy threats: *surveillance*, *appropriation*, and *distortion*. Their related privacy goals are: *data unlinkability*, *purpose specification*, *transparency* and *integrity*. The generator raise no warning, as all the identified privacy threats are addressed. Following is the status of security controls, as generator reported:

- Data Unlinkability
 - Number of provided security controls: "8",
 - Number of Applicable ones: "6",
 - Number of Implemented ones: "2",
 - Number of Not Implemented ones: "4",
 - Likelihood Level: "3.3",
 - Protection Level: "1.7".
- Minimization
 - Number of provided security controls: "7",
 - Number of Applicable ones: "5",
 - Number of Implemented ones: "4",
 - Number of Not Implemented ones: "1",
 - Likelihood Level: "1",
 - Protection Level: "4"
- Purpose Specification
 - Number of provided security controls: "2",
 - Number of Applicable ones: "2",
 - Number of Implemented ones: "2",
 - Number of Not Implemented ones: "0",
 - Likelihood Level: "0",
 - Protection Level: "5"
- Purpose limitation
 - Number of provided security controls: "1",
 - Number of Applicable ones: "1",
 - Number of Implemented ones: "1",

- Number of Not Implemented ones: "0",
 - Likelihood Level: "0",
 - Protection Level: "5"
- Transparency
 - Number of provided security controls: "3",
 - Number of Applicable ones: "3",
 - Number of Implemented ones: "2",
 - Number of Not Implemented ones: "1",
 - Likelihood Level: "1.7",
 - Protection Level: "3.3"
- Intervenableity
 - Number of provided security controls: "4",
 - Number of Applicable ones: "4",
 - Number of Implemented ones: "1",
 - Number of Not Implemented ones: "3",
 - Likelihood Level: "4",
 - Protection Level: "1"
- Lawfulness
 - Number of provided security controls: "3",
 - Number of Applicable ones: "3",
 - Number of Implemented ones: "3",
 - Number of Not Implemented ones: "0",
 - Likelihood Level: "0",
 - Protection Level: "5"
- Accountability
 - Number of provided security controls: "3",
 - Number of Applicable ones: "3",
 - Number of Implemented ones: "3",
 - Number of Not Implemented ones: "0",

- Likelihood Level: "0",
- Protection Level: "5"
- Storage limitation
 - Number of provided security controls: "2",
 - Number of Applicable ones: "2",
 - Number of Implemented ones: "2",
 - Likelihood Level: "0",
 - Protection Level: "5"

Assessing Compliance with the DPIA_{privacy} The *Privacy BCP Checker* report no warning as for each privacy goal, at least one tactic is implemented.

5.3.4 Investigate vulnerabilities

To identify the vulnerabilities, we use the National Vulnerability Database (NVD).⁷ The NVD is the U.S. government repository of standards-based vulnerability management, which includes databases of security checklist references, security-related software flaws, misconfigurations, and impact metrics. It specifies the vulnerable object (either an application, an operating system, or a hardware), by the name of its vendor and product, and its version. We use the NVD to check whether the employed supporting assets, security technology or PETs are vulnerable. The NVD offers an API for organizations to query and ingest vulnerability data [BO].

The controller, when possible, has provided the supporting assets (see Section 5.2.3), security technologies (see Section 5.3.2), and PETs (see Section 5.3.3) by specifying the name of the vendor, product, and version. They are reported in the document *NVDInput* document. We have a component called *NVD Checker*. The checker gets the *NVDInput* document, and queries the NVD API with the name of vendors, if any occurrence, it retrieves the record(s) where the word is found in the vulnerability description. Once the checker has the vulnerability(s) related to the vendor stored locally, it queries that with the product name and version. If it finds any matches, it retrieves: CVE ID, exploitability score, and impacted security goal(s). CVE IDs are identifiers for known vulnerabilities. when making a request to the NVD API, one can specify the publication period when the CVE is added to the data base, by specifying the starting and end date. It is not necessary to provide both start and

⁷<https://nvd.nist.gov/general>

end dates if the goal is to retrieve all CVE after a certain date, or up to a certain date.

Exploitability score reflects the ease that a vulnerability can be exploited; the higher the score, the easier to exploit the vulnerability. While, likelihood level reflect how probable it is that a vulnerability can be exploited; the higher the score, the more probable for the vulnerability to be exploited. We can say that, approximately, the likelihood level is equal to exploitability score. When the score relates to a supporting asset, we use the score as the likelihood of compromising the related goal. While, when the score relates to security/privacy technologies—that are meant to protect the system—the exploitability score impacts their level of protection. We consider the protection level to be 0 when the security control is vulnerable. Note that, where provided, we use CVSS version 3.0.⁸ The *NVD checker* reports the above mentioned information in a document, called *Captured Vulnerabilities*. The document *Captured Vulnerabilities* is an inputs to address problem P_{risk} (see Section 2.3.1).

5.3.4.1 Application of the Step on the Running Example

NVD Checker gets the following inputs from the *NVD Input*:

- Vendor: "HP", Product: "fax-ready HP OfficeJet inkjet printer", Version: "";
- Vendor: "ownCloud", Product: "server", Version: "10.0.1";
- Vendor: "Auth0", Product: "Auth0.js", Version: "8.10.1";
- Vendor: "Microsoft", Product: "Active Directory Federation Services", Version: "4.0";
- Vendor: "Cisco", Product: "firepower management center", Version: "6.4.0";
- Vendor: "Juniper Networks", Product: "Junos Space", Version: "15.2";
- Vendor: "PulseSecure", Product: "Pulse Connect Secure", Version: "43";
- Vendor: "Microsoft", Product: "Azure Security center", Version: "".

It queries the NVD API by the vendors and queries its results by the name of product and version. It reports the followings, note that we have normalized exploitability scores to 5:

⁸Please refer to <https://www.first.org/cvss/specification-document> for more information on how the scores are evaluated.

- CVE-2018-5925: *fax-ready HP OfficeJet inkjet printer* allows remote code execution that impacts *confidentiality*, *integrity* and *availability*, with exploitability Score of 1.3;
- CVE-2017-9338: *ownCloud Server* suffers from an inadequate escaping that leads to cross site scripting that impacts *confidentiality* and *integrity*, with exploitability Score of 1.6;
- CVE-2018-6873: *Auth0 authentication service* allows privilege escalation because the JWT audience is not validated that impacts *confidentiality*, *integrity* and *availability*, with exploitability Score of 2.9;
- CVE-2018-16794: *Microsoft ADFS 4.0 Windows Server 2016 version 4* suffers from SSRF vulnerability that impacts *integrity*, with exploitability Score of 2.9;
- CVE-2020-3285: *CISCO firepower management center* suffers from a logic error with Snort handling of the connection with the TLS 1.3 policy and URL category configuration that impacts *integrity*, with an exploitability Score of 2.9;
- CVE-2017-2310: *Juniper Networks Junos Space versions to 15.2* suffers from a firewall bypass vulnerability in the host-based firewall of Juniper Networks Junos Space that impacts *integrity*, with an exploitability Score of 2.9;
- CVE-2019-11543: *Pulse Connect Secure* suffers from cross site scripting in the admin web console that impacts *confidentiality* and *integrity*, with exploitability Score of 1.8;

Note that we have normalized the exploitability score in scale of 1 to 5.

5.3.5 Compliance of Access Control Policies

Controllers cannot ensure being compliance with the requirements of the GDPR only by defining and enforcing access control policies—they need to comply with the GDPR requirements. If not, the controller risks being non-compliant. To avoid such risks, we have used the tool proposed by [GRS17, RS17], introduced in Section 4.6. The control needs to write the *bridge structure* (see Section 4.6) from the *User-specified Access Control* file (see Section 5.2.3). The bridge structure will be input into the employed tool to be checked. The tool reports if there is any non-compliance occurs.

5.3.5.1 Application of the Step on the the Running Example

The controller defines the following bridge structure from the access control policies, identified in the MSC (see Figure 5.3), when ITOrg is the controller, ACME is the processor and employees are the data subjects. The access control could be read, write, update and transfer.

$$\begin{aligned}
& ITOrg \wedge a = r \wedge Profile \wedge Employee \vee \\
& ITOrg \wedge a = w \wedge Profile \wedge Employee \vee \\
& ITOrg \wedge a = u \wedge Profile \wedge Employee \vee \\
& ITOrg \wedge a = r \wedge Profile \wedge ITOrg \vee \\
& ITOrg \wedge a = r \wedge Fin_Profile \wedge ITOrg \vee \\
& ITOrg \wedge a = w \wedge Fin_Profile \wedge ITOrg \vee \\
& ITOrg \wedge a = u \wedge Fin_Profile \wedge ITOrg \vee \\
& ITOrg \wedge a = r \wedge Fin_Profile \wedge Fin_Dep \vee \\
& ITOrg \wedge a = w \wedge Fin_Profile \wedge Fin_Dep \vee \\
& ITOrg \wedge a = u \wedge Fin_Profile \wedge Fin_Dep \vee \\
& ITOrg \wedge a = r \wedge Fin_Profile \wedge ACME \vee \\
& ITOrg \wedge a = r \wedge Salary \wedge ACME \vee \\
& ITOrg \wedge a = w \wedge Salary \wedge ACME \vee \\
& ITOrg \wedge a = u \wedge Salary \wedge ACME \vee \\
& ITOrg \wedge a = r \wedge Salary \wedge Fin_Dep \vee \\
& ITOrg \wedge a = r \wedge Salary \wedge Employee \vee
\end{aligned} \tag{5.1}$$

The controller inputs the bridge structure into the automated tool to check for possible non-compliance access control policies. The tool reports a non-compliance, as the controller does not grant Transfer access to data subject Employee. From the security point of view, this does not make any problem. However, the GDPR requires such access to be granted (article 20).

5.3.6 Modeling Risk

To model risks, we have extended the RiskML tool, introduced in Section 4.5, to generate the risk model automatically. We have explained the components that the

RiskML relies on to build the model (see Section 4.5). Following we indicate how they are translated into our context:

- situation captures the security controls; privacy tactics; if indicated, their related technologies; and vulnerable supporting assets;
- indicator gets the value 0 when the corresponding *Situation* does not hold, and 1 otherwise;
- event captures the security/privacy goal that the related situation can compromise if not implemented;
- goal capture the security/privacy goal that the related situation is to address.

These components are connected to one another with the following relations: Indicate (i, s), Expose (s,e,w), Expose (e,e,w), Protect (s,e,w), Impact(e,g,w); where weight on the relation *expose* indicates the likelihood of the event to happen, and on relation *protect* indicates how the likelihood decreases if the corresponding situation holds. When there is more than one situation connected to an event—either with *expose* or *protect* relation—we adjust the RiskML tool to sum the values of the relation (instead of taking the maximum). That is because, we consider that each security control/privacy tactics contribute equally.

First, we want the model to represent the system as-is. To model the system as-is, we need the implemented and not-implemented security controls and privacy tactics, and employed vulnerable supporting assets—from which we only need the vulnerable one that impacts the system’s security—and their related threats and goals. They are captured with the following documents: *Security Risk Summary*, *Privacy Risk Summary*, and *Captured Vulnerabilities*. Once the controller observed the system as-is and the risk level, we want him to observe how the risk level changes if the system has been configured differently by performing what-if analysis that RiskML provides. What-if analysis helps the controller to make an informed decision on how to configure the system for a data processing in question to decrease the risk level to the rights and freedoms of data subjects. We provide the possibility of performing the following what-if analysis:

- what if the controller had implemented the overlooked security controls?
- what if the controller had implemented the overlooked privacy tactics?
- what if the controller had not employed the vulnerable security/privacy technology or the vulnerable supporting asset?

To prepare the input for the RiskML tool to model the system as-is and provide the above-mentioned what-if analysis, we introduce a component called *Static XML Generator*. The Generator gets as input the two reference models: *Security Reference Model* and *Privacy Reference Model*, stored in *ControlReferenceModel_DB* and *StrategiesReferenceModel_DB*, respectively. These models contain all the security controls and privacy tactics that controllers could implement. The generator models the security controls and privacy tactics once as they are all implemented, that is, with the *protect* relation; and then as they are not, that is, with the *expose* relation. We call the situation with relation *expose*, *expose-situation*; and with relation *protect*, *protect-situation*. All the indicators are set to 0. The generator outputs a model called *Static XML file*. The file will be regenerated whenever either of the tables gets updated. Figure 5.8.a represents a *Static XML File* where the two controls appear both with *expose* and *protect* relation. The weights of the relations will be set when the model get customized for the system in question; and the indicators are set to 0.

```

1  { "Goal": ==> Goal, and
2    Event==> "Compromised+GoalName"
3  [
4    { "Tactic/Control": "", ==> Situation
5      "baseline": [{ "Low": [""]},
6                  { "Moderate": [""]},
7                  { "High": [""]}],
8      "question": "",
9      "Answer": "", ==> Used to set indicators and Relation.
10     "OtherGoal": "" ==> "Yes/Partially Applicable" to Protect and "No" to Expose.
11   }
12 ],
13 "Likelihood":
14 { "Tactic/Control":
15   { "total": "",
16     "Applicable": "",
17     "Implemented": "",
18     "NotImplemented": "",
19     "LikelihoodLevel": "", ==> Expose relation Weight.
20     "ProtectionLevel": "" ==> Protection Relation Weight.
21   }
22 }
23 }
24 -}

```

Figure 5.6: Annotated Security/Privacy Risk Summary Document to Extract RiskML Model.

To customize the *Static XML file* to represent the data processing in question, which is called *Customized XML File*, we use another component called *customized XML Generator*. The generator gets *Security Risk Summary* and *Privacy Risk Summary*. Wherever the response is *Yes* or *partially implemented*, the generator set the indicator of related *protect-situation* to 1; and when the answer is *No* sets the indicator of

```

1 [
2 {
3   "Product": "VendorName+ProductName+Version", ==> Situation
4   "CVEID": "", ==> Event
5   "ImpactedSecurityGoal": [], ==> Goal
6   "ExploitabilityScore": "" ==> Decrease protection level accordingly
7 }
8 ]

```

Figure 5.7: Annotated Captured Vulnerabilities Document

the related *expose-situation* to 1. When the answer is *Not Applicable*, the generator drops the indicator—as they do not contribute neither in risk level calculation nor to what-if analysis. The indicator of protect-situation related to not-implemented applicable security controls and privacy tactics remain 0—as they are not contributing to protecting the information system, but we keep them for the what-if analysis. Figure 5.6 represents JSON schema of the security/Privacy Risk Summary (which are similar except for the part highlighted in blue) to represent how each component of the JSON file translates to RiskML components.

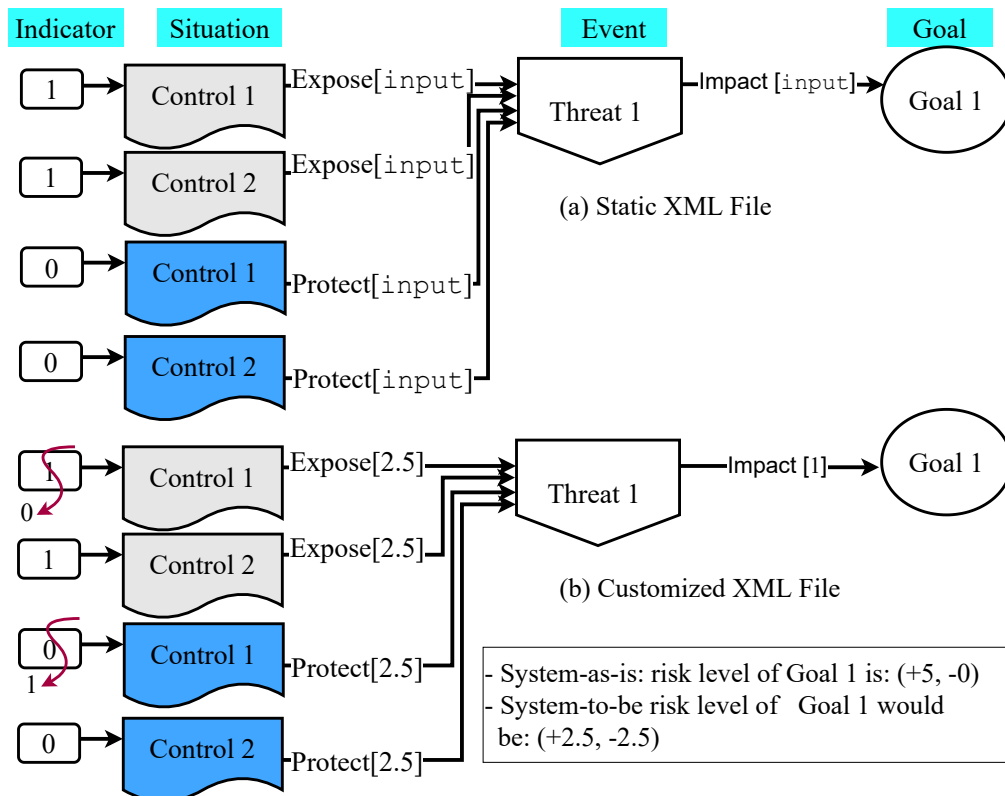


Figure 5.8: An example of Customized XML File.

The generator also gets document *Captured Vulnerabilities*, to model the vulnerable supporting assets and security/privacy technologies. The vulnerable supporting assets expose the system to a threat, so they will only be represented with expose-situation, and the controller can see how the risk level changes if the vulnerable supporting asset has not been used (that is, when a secure supporting asset is used). Figure 5.7 shows how the RiskML translates the inputs' entries of document *Captured Vulnerabilities*.

To perform what-if analysis, the controller only needs to change the value of indicators, and see instantly how the risk level changes.

Figure 5.8.b represents a system where none of the two controls are implemented, so the indicators of their expose-situation are set to 1. The model keep their related protect-situation, with indicators set to 0, to perform what-if analysis. Their relation expose is weighted 2.5, as we assume that the controls contribute equally; and the impact of data processing on *Goal 1* is 1. Since, none of the controls are implemented the risk level of the system-as-is is $(+5, -0)$. But, if the controller has implemented *control 1*, the risk level would have been $(+2.5, -2.5)$. Note, when the controller change the indicator of a expose-situation, the indicator of its related protect-situation will change accordingly.

5.3.6.1 Application of the Step on Running Example

The *Customized XML File* related to the running example is generated using the following documents: *Security Risk Summary* (see Figure 5.4), *Privacy Risk Summary* (see Figure 5.5), and *Captured Vulnerabilities* (see Section 5.3.4). Figure 5.9 and 5.10 show the security and privacy model, respectively. To keep the models clean, we dropped the impact value—which is 5—on *impact* relations. The models shall be connected, we divided them in two, for readability purpose.

Figure 5.9 shows the risk model related to security goals. The evaluated risk levels of each goal by the are as follows:

- Confidentiality: $(+3.8, -0.6)$;
- Integrity: $(+4.7, -0.6)$;
- Availability: $(+4.9, -0)$.

The protection levels are decreasing and likelihood levels are increased respecting the evaluated ones by the *Control Questionnaire*, presented in Section 5.3.2.3, due to the vulnerable supporting asset and security technologies. To give an example of

what-if analysis, consider if the controller would have used an invulnerable printer, instead of the *fax-ready HP OfficeJet inkjet printer* with likelihood level 3.2, the risk level would be as follows:

- Confidentiality: $(+0.6, -0.6)$;
- Integrity: $(+1.5, -0.6)$;
- Availability: $(+1.7, -0)$.

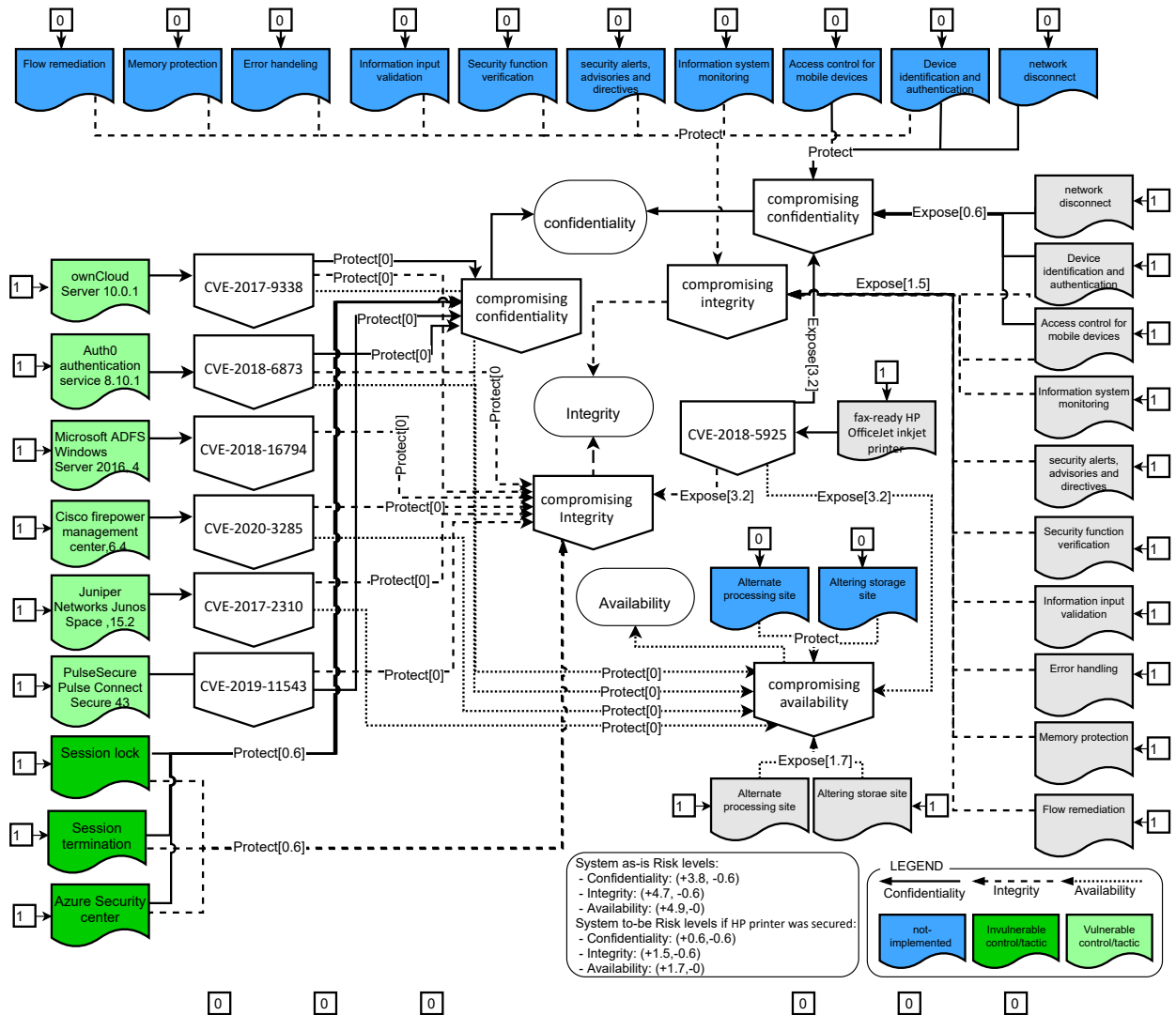


Figure 5.9: Security Risk Model of the Running Example.

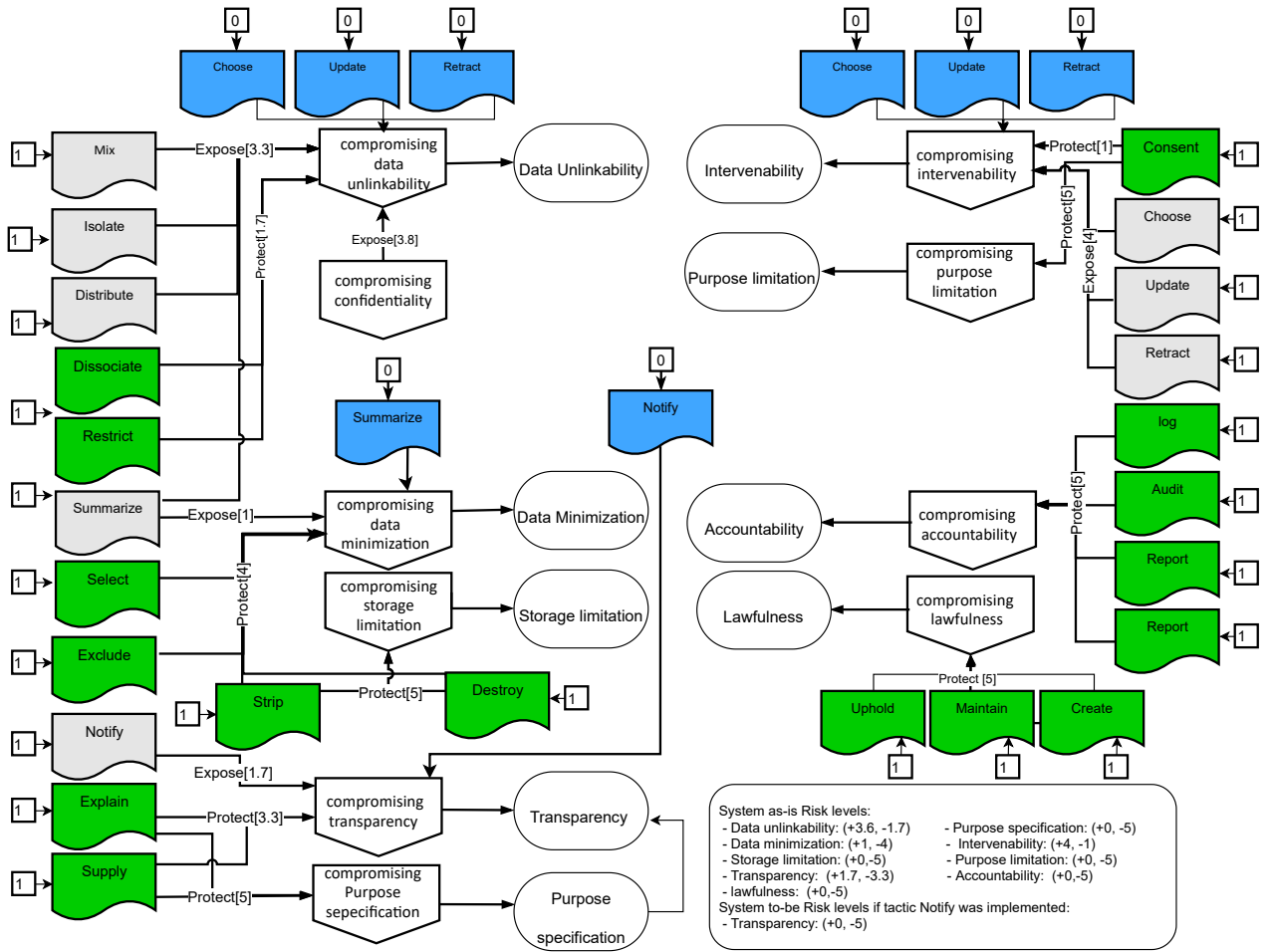


Figure 5.10: Privacy Risk Model of the Running Example.

Figure 5.10 shows the risk model related to privacy goals. The evaluated risk levels of each goal are as follows:

- Data unlinkability: (+3.6, -1.7);
- Data minimization: (+1, -4);
- Intervenable: (+4, -1);
- Purpose specification: (+0, -5);
- Storage limitation: (+0, -5);
- Transparency: (+1.7, -3.3);

- Purpose limitation: $(+0, -5)$;
- Accountability: $(+0, -5)$;
- lawfulness: $(+0, -5)$.

The Figure show that the event *compromising confidentiality* impacts also privacy goal *Unlinkability*. If the controller had implemented a technology to meet privacy tactics *Notify*, the risk level of privacy goal *Transparency* would become: $(+0, -5)$.

5.4 Related Work

This chapter discusses related privacy risk assessments, data protection, privacy by design, and data protection impact assessment.

5.4.1 Privacy risk Managements Approaches

Regardless of the size, structure or nature of an organization, processing personal data unavoidably gives rise to risk [IC10]. Privacy Risk Analysis (PRA) is required when the system relies on the processing of personal data, because of the variety of privacy breaches that could arise. Conducting PRA help to capture these breaches in the early stage and introduce proper countermeasures [LMW10, Pep14]. Although privacy risk analysis intersects with security risk analysis, there are security issues unrelated to privacy (e.g., the confidentiality of trade secrets) just as there are issues unrelated to security [BGL⁺17]. The objective of a privacy risk analysis is mostly to identify the privacy harms for a system in a given context and to assess the associated risks, which are generally measured in terms of *likelihood* and *impact* [DLM16]. The authors in [BGL⁺17, CNI12a, DWS⁺11, FGK13, NIS] have focused on PRA; following we discuss them further.

CNIL provides an implementation of a risk management approach in the context of privacy [CNI12a] that is compliant with international standards for risk management, including ISO31000. They stated that in the area of privacy, the only risks to consider are those that the processing of personal data poses to privacy. Those risks are composed of one feared event—things to avoid—and the threats that make it possible. They introduce five feared events: unavailability of legal processes, change in processing, illegitimate access to personal data, unwanted change in personal data, the disappearance of personal data. For a feared event to occur, one or more risk sources—that could be either human, accidentally or deliberately, or

non-human, act on the supporting assets that include: hardware, software, networks, people, paper media, and paper transmission channels. To evaluate likelihood they consider the vulnerability of supporting assets—various information system components—capabilities of risk source and existing measures. And to evaluate the impact they consider the identifiability level of personal data and the prejudicial effect of each feared event on the individuals. In our methodology, we also assess the vulnerability of the supporting assets and security controls to identify possible threats automatically.

NISTIR 8062 [BGL⁺17] defines privacy engineering as a specialty discipline of systems engineering focused on achieving freedom from conditions arising from processing personal data that can create problems for individuals with unacceptable consequences. It aims to provide a degree of precision to encourage the implementation of measurable controls for managing privacy concerns and to help system designers and engineers working with policy teams bridge the gap between high-level privacy principles and their implementation within systems. As security concerns, some privacy concerns arise from unauthorized activity that could impact security goals—confidentiality, integrity or availability (known as CIA)—of the information system; privacy concerns also can arise from authorized processing of information about individuals. As security goals are means to categorize capabilities and controls to achieve security outcomes, so do privacy goals. They introduce the following privacy goals: *disassociability* to enable reliable assumptions, *predictability* to enable granular administration of personal data, and *manageability* to enable personal data processing without associating them to individuals or devices beyond the processing requirements. NISTIR 8062 believes that the terms “*threat*” and “*vulnerability*” fails to capture the essence of many privacy problems for individuals. So, they introduce the term “*problematic data action*” which means a data action that impacts individuals. In [NIS], NIST lists some problematic data actions, such as: *appropriation*, *distortion* and *induced disclosure*; and mapped them to privacy concerns that they could raise. The problem that mentioned problematic data actions lead to are *loss of trust*, *discrimination* and *loss of autonomy*, respectively. Problematic data action plays the same functional role in framing the adverse event as making threats in the information security risk model; it can be expressed as the *likelihood* that a vulnerability will be exploited by a threat *impact* of such occurrence. *Likelihood* is the probability that a data action will become problematic for a representative or typical individual whose personal data is processed by the system; users’ perceptions of a data action is critical to determining likelihood; some ways to evaluate it that includes: using customer demographics, extrapolating from information in similar scenarios, and conducting focus groups or surveys to learn about users’ privacy concerns. *Impact* is the magnitude of cost or harm from the problematic data action. The fact that only individuals can directly experience a privacy problem is especially

challenging. NISTIR 8062 suggest using various other costs to help account for the individual impact, such as: legal compliance costs for individuals, reputational costs leading to loss of trust, and mission failure cost such as reluctance to use the system or service.

In our methodology, we have mapped the NIST problematic data actions to the privacy risks introduced in Recital 75, to capturing the privacy risk are not easy due to being abstract.

ISO/IEC 29100:2011 [291] provides a high-level framework for protecting personal data within information and communication technology systems (ICT). The ISO introduces the components that relate to privacy and the processing of personal data in ICT systems, such as actors and roles, interactions among the actors, privacy policies, and privacy controls. It introduces privacy principles which are driven from existing principles developed by many states, countries and international organizations, namely: consent and choice; purpose legitimacy and specification; collection limitation; data minimization; use, retention and disclosure limitation; accuracy and quality; openness, transparency and notice; individual participation and access; accountability; information security; and privacy compliance. These principles intersect with the GDPR *Data Processing Principles*, articulated in article 5.

As most of the newly deployed IT products and services rely on personal data, not taking proper measures leads to various privacy breaches. To ensure that such risks are properly understood and addressed, a growing recognition is a privacy impact assessment (PIA). Authors in [DLM16] discuss that, although there is a large body of contributions on PIAs and several PIAs for specific products have been published. They do not precisely define how the technical part of the PIA, that is, Privacy Risk Analysis, should be performed. As such, they propose a framework and methodology for conducting a rigorous and systematic PRA, called PRIAM. The methodology consists of two phases: the Information gathering and the Risk assessment phase. The first aims to gather all the relevant information. The component categories and lists of attributes are helpful to this respect. The framework relies on seven components, including: *risk source* (e.g., insider) that is any entity whose actions may directly or indirectly, intentionally or unintentionally lead to privacy harms; *privacy weakness* (e.g., software error) that is a weakness in the data protection mechanisms; *feared event* (e.g., excessive data collection) that is an event that occurs as a result of exploiting one or more privacy weaknesses; and *privacy harm* (e.g., mental or psychological harms) that is the negative impact resulting from one or more feared events. Each component have different attributes, which refer to the aspects of the component that affect privacy harms. *Motivation*, *irreversibility*, *exploitability*, and *victim of the harm* are examples of attributes for the above mentioned components, respectively. The second phase aims to use the values of the attributes to compute

the risk levels, which are pairs (severity, likelihood), for each privacy harm. This computation is based on harm trees which are used to establish a relationship among privacy weaknesses, feared events and harms. The root of the tree denotes privacy harm, and nodes denote privacy weaknesses exploited by the most likely risk source for the particular harm and represented by pairs (privacy weakness, risk source). They calculate the likelihood of privacy harms according to the likelihood calculated for its feared events, which is done based on values of their attributes. The authors state that severity is an inherent measure of the damage caused by harm, it cannot be reduced, and the only factor in controlling is the likelihood. Therefore, the most appropriate set of countermeasures is one that brings the risk level of all harms associated with the system below a given acceptable level and at the same time leads to minimal costs for implementation.

Similar to [DLM16], authors in [AS17] discuss that for a PIA to be holistic and practical, it needs to be complemented by an appropriate PRA. They propose a methodical approach for identifying and analyzing potential privacy risks, based on a conceptual model; built upon [DLM16] and [CNI12a], by refining the concepts, risk factors and relationships among these factors. They emphasize on the importance of data-management models where they use *Abstract Personal Data Lifecycle* (APDL) Model to describe processing activities better. That are abstractly represented in eight stages: *Initiation, Collection, Retention, Access, Review, Usage, Disclosure* and *Destruction*. They refer to Solove’s taxonomy [Sol05] to understand the specific characteristics of adverse privacy events. Adverse events are characterized according to the nature of processing operations in each stage of the lifecycle. For instance, in the *collection* stage, adverse events are related to how personal data is collected, such as surveillance and interrogation—they are more related to primary assets than supporting assets. Adverse events are associated with privacy harms that are classified into: physical, economic or financial harms, mental or psychological harms, harms to dignity or reputation, and societal or architectural harms, as in [DLM16]. To capture possible privacy harm, they analyze vulnerabilities to primary assets, i.e., data. Then they capture threat events that occur as a result of the exploitation of one or more vulnerabilities. They consider identifying and analysing vulnerabilities of the supporting assets as a part of security risk analysis to protect primary assets. While, there are privacy risks unrelated to security [BGL⁺17], they are closely relate [oMB16]. Indeed, security is typically recognized as one of the FIPPs [oMB16]. There is a clear recognition that confidentiality of personal data plays an important role in the protection of privacy [BGL⁺17]. Accordingly, in our methodology, we capture privacy risks and consider the security risks that could lead to harm to the rights and freedoms of data subjects.

The LINDDUN methodology [DWS⁺11] addresses the lack of a systematic approach to model privacy threats, elicit privacy requirements, and instantiate privacy-enhancing

technologies. Each letter of “LINDDUN” stands for a privacy threat type—that are: Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Content Unawareness, Policy, and consent noncompliance—obtained by negating a privacy property— Unlinkability, Anonymity and Pseudonymity, Plausible deniability, Undetectability and unobservability, Confidentiality, Content awareness, and Policy and consent compliance. LINDDUN provides an extensive catalog of privacy-specific threat tree patterns [WSJ14] that can be used to detail the threats. Finally, LINDDUN provides a list of privacy solutions to mitigate elicited threats. In our methodology, we have used their mapping of privacy properties to PETs.

5.4.1.1 Discussion

The GDPR introduces a risk-based approach for determining which technical and organisational measures are appropriate in the given situation [VvdB17]; DPIA is considered to be a risk management tool [VDGR16] which considers risks to the rights and freedoms of data subjects. We aimed to propose a methodology that assist controllers to conduct a DPIA. As such, we studied the state-of-the art to learn about the privacy risk management approaches. From the studied approaches, we have learnt: to consider vulnerabilities of supporting assets, security technologies and privacy enhanced technologies (as risk sources could act on them on which the primary assets (being personal data) rely [CNI12a]), that is unlike [AS17] which consider them as security risks and unrelated to privacy—indeed, security and privacy intersects; about problematic data actions [NIS] through which we identify privacy risks.

5.4.2 Data Protection Impact Assessment

Privacy Impact Assessment (PIA) has gradually developed from the 1990s onward [VDGR16], and adopted in Australia, Canada, New Zealand, and the United States. The UK introduced the first PIA methodology in Europe in 2007. The European Data Protection Board (EDPB) set general requirements for PIAs for the RFID [Artc] in 2009, and smart metering [Artb] in 2012. It has also mainly been studied by academic works, e.g., [Cla09, Wri12, OS14, Cla99, Spi12, CK13]. D.Wright defines PIA as “a methodology for assessing the impacts on the privacy of a project, policy, program, service, product or other initiatives which involves the processing of personal information and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimize negative impacts” [WdH12]. In his book, he has proposed a sixteen-step optimized PIA process based on a review of various existing PIA methodologies. When these works were developed, conducting

a PIA was not a legal obligation. The UK Information Commissioner’s Office (ICO) introduced it as “a tool which can help organizations identify the most effective way to comply with their data protection obligations and meet individuals’ expectations of privacy” [ICO14]; and the French Commission Nationale de l’Informatique et des Liberties (CNIL) refer to PIA as the process that “[..] data controllers who wish to demonstrate their compliance approach and the controls they have selected, as well as for product providers wishing to show that their solutions do not breach privacy” [CNI15].

PIA was not a mandatory assessment until the GDPR made it. It requires controllers to conduct a Data Protection Impact Assessment (DPIA), stipulated by article 35; when data processing is likely to result in a high risk to the rights and freedoms of natural persons. Article 35(7) provides a minimum standard for carrying out the DPIA, and does not lay down any further requirements. It is unclear how to implement it [AS17, CFKA18, VDGR16, DLM16, BFH+16, DLM17, vPH17, MH15]. Data Protection Authorities have published some guidelines and approaches; they suffer from limited assistance [VK18]. National privacy authorities—such as CNIL [CNI18] and ICO [ICO18]—have proposed guidelines to conduct a DPIA.

EDPB proposes an iterative process for carrying out a DPIA [Arta] consisting of the following seven steps organized in a cycle: (1) description of the envisaged processing, (2) assessment of the necessity and proportionality, (3) data protection measures already envisaged, (4) assessment of the risks to the right and freedoms of data subjects, (5) data protection measures envisaged to address the risks, (6) documentation, (7) monitoring and reviewing. Our proposed methodology is organized in three steps, namely: Processing Analysis, Risk Analysis, and Run-time Analysis. Each step generates a document. These steps cover those by the EDPB, as follows: Processing Analysis corresponds to steps (1) and (2); Risk Analysis to steps (3), (4), and (5); Run-time Analysis to step (7); and the three documents generated by our tool covers step (6).

ICO provides a self-assessment toolkit [ICO], which offers checklists for different roles, namely controller and processor. The toolkit helps to lead a discussion to find out what needs to be done and keep people’s personal data secure. On the other hand, CNIL introduces a tool [CNI] that requires the user to answer several questions, which are grouped in three categories: 1) to describe the context of processing, e.g., applicable standards, data types involved, supporting assets; 2) fundamental principles, e.g., whether the involved data is proportionate to the purpose, whether the data are accurate, storage duration; 3) risks, e.g., existing controls, possible risks, and the likelihood and impact. Then, the tool returns a visual representation of the collected data that includes the considerations of the Data Protection Officer (DPO) and the Data Subjects (or their representatives). Both of these

works resemble a check-list—which is not an assessment⁹—they do not provide effective assistance as is the case of our tool. Our tool assists the user in evaluating risk in two phases by assessing the implemented security countermeasures and the vulnerabilities in the supporting assets and implementing security countermeasures.

The authors of [BFH⁺16] use a three-stage process to conduct the DPIA, namely: preparation, evaluation, and report and safeguard. They use the Standard Data Protection Model (SDM) [Con17] to demonstrate compliance with data protection requirements and identify appropriate safeguards. SDM systematizes technical and organizational measures to protect the rights of the data subjects based on protection goals. The authors use a catalog of data protection measures developed by the technical working group of German data protection authorities (AK Technik). These works show the requirements and steps to comply, while our work assists the user to meet the DPIA requirements and be compliant.

The authors in [CFKA18] use UML class diagrams to specify crucial requirements underlying various aspects of a DPIA, such as consent and necessity. Their focus is to integrate security and privacy requirements engineering processes into a DPIA and understand how a previously developed tool for risk analysis of UML diagrams can be effectively used in this context.

In [SWBS19], authors have introduced a tool-supported formal method to verify whether privacy properties are met or not. The authors believe that using such a tool makes the validity of the DPIA more understandable and manageable; also, it verifies whether the DPIA performed by the controller has captured the risks raised from excessive data collection and unauthorized purposes. While using such a tool is helpful, they still cannot capture all the DPIA requirements and instead focus on purpose and consent.

PIA Evaluation and Grading System (PEGS) evaluate PIA reports according to some criterias [WR13]. The PEGS wights the criteria according to their contribution towards a successful PIA conduction. It weighted the *Information flow mapping* ‘2’; and identification of privacy risks and their impacts, identifying solutions to treat risks ‘3’. None of the previous works has considered them, while in our methodology, we ask controllers to draw information flow where they are assisted in identifying the privacy risks and later to identify treatments.

The authors in [ACDC⁺15] offer a tool-supported DPIA for Cloud Service Provider (CSP). They have two questionnaires: one to assess whether the DPIA is necessary and another to establish the effect of interactions among data subjects and CSPs on their rights to data protection. The questions have some pre-defined answers, which

⁹<https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2017/gdpr-what-a-data-protection-impact-assessment-is-and-isnt>

are associated with privacy indicators and weighted according to the impact they have on them. A global privacy indicator is then calculated based on the indicators. While we share some similarities in the risk analysis phase, our tool is agnostic concerning the technology used to implement the data processing activities. The Risk Analysis step of our methodology is parametric concerning the particular technique used for risk evaluation.

The authors of [ASRJ18] propose UML-based security and privacy analysis. They annotate the UML with the security requirements and check if they are satisfied using UMLsec. To specify the level of privacy, they have extended the Privacy Level Agreement (PLA) to include the following four privacy preferences: purpose, granularity, visibility, and retention. A PLA is an appendix to a service level agreement and provides a structured means to specify privacy preferences and data security requirements. The authors map the harmful activities, introduced in [Sol05], to privacy targets, introduced in [OS14], privacy threats and appropriate checks. Thus, by identifying the harmful activities in the diagram, they react accordingly. To evaluate impact, they extend the mapping to the privacy target to identify what has to be protected and its impact on the data subject and data processor. The authors do not consider specific likelihood, as they believe that if a privacy threat exists, we control it. They also associate security controls with the mapping. The security controls are based on the NIST 800-53r4, ISO 27001, and German IT baseline. Although we share a similar approach, we acknowledge the fact that privacy and security are inseparable; thus, we check whether the security controls or supporting assets are vulnerable. Moreover, we check compliance with the access control policy, as having them implemented cannot guarantee compliance. Lastly, DPIA is not a one-time activity rather it has to continue as long as the life-cycle of the data processing; which the authors of [ASRJ18] have not considered.

After evaluation of nine commonly used PIA methods and guidelines, authors in [VK18] indicated area that needs further research and success factors that are: tools to automate risk identification from data flows, and automatically create the PIA report, exploring privacy risks from the organization perspective, reconsidering the data process and deciding not to process some data elements if not critical for the desired purpose should be espoused, providing privacy controls' lists. The DPIA needs to be adequately tool-supported, such that data input in one step can be used to support reasoning and analysis in others [CFKA18]. Our methodology is tool-supported, it covers the aforementioned needs and factors in its different steps.

5.4.2.1 Discussion

The guideline published by the European Data Protection Board (EDPB) on the DPIA provided more explanation on how to conduct one [Arta] that the article 35 of the GDPR, yet it did not clarified the steps and provided no assistance to the controllers. The UK [ICO18] and French data protection authority[CNI18] have also offered tools that show the steps and what to consider, without providing assistance to controllers. Learning about these legal bodies motivated us to learn also about the academic works on the subject, such as [BFH⁺16, CFKA18, ASRJ18, SWBS19, ACDC⁺15]). These works too lack to either provide assistance (they work more like a checklist), include all steps of the DPIA (e.g., monitoring), or be applicable to all domains.

Therefore, we proposed a methodology that assist controllers in all the steps of the DPIA, from identifying the data type required for the data processing to capturing the privacy and security risks. Our methodology is applicable in different domains. It offers security and privacy reference model to assess system in question and propose treatments for the captured risks; the model can be updated, if needed. For example, we have build another reference model to apply the methodology on OAuth/OIDC solutions (see Section 6).

5.5 Conclusion

Controllers need to evaluate risks to rights and freedoms of data subjects, and introduce treatments to preserve their rights, ensure an ongoing confidentiality, integrity, availability and resilience of processing systems and services, and respect data processing principle. When the processing is likely to results in high risks to data subjects' rights and freedoms, controllers need to conduct a DPIA.

In this chapter, we discussed that even if a DPIA is not required for a given data processing—which is mostly required—controllers need to identify and evaluate privacy and security risks—the former is not easy to identify—respect data subjects rights and data processing principles. So, they do not risk to be non-compliance. Controller need assistance to comply with these requirements. We presented our assisted methodology to help controllers in conducting a DPIA. The methodology has three steps: *Processing Analysis*, *Risk Analysis* and *Run-time Analysis*. We have presented the first two steps of our methodology. The first step is to collect required information about the organization in questions and the data processing it conducts. The second step is to assess the level of security and privacy of the data processing in question and evaluate the security and privacy risks. The steps are semi-automated as it requires inputs from controller (shown in Figure 5.1). We plan to investigate

how to combine data analytic techniques with selected monitoring tools—such as those for Inventory Management (IM) and Security Information and Event Management (SIEM)—to implement the third step, namely *Run-time analysis*—cf. Figure [5.1](#). We also plan to develop a tool that supports our methodology. In this thesis, we only implemented some parts to ensure whether it is feasible to automate them.

Chapter 6

Application Of Methodology On OAuth/OIDC-based Services¹

The growing importance of financial services and the regulatory push by the Directive (EU) 2015/2366 on payment services (PSD2) to share user's financial data with third-party services have made the market more competitive. Although that brings a range of economic opportunities, it comes together with risks such as loss or theft of personal data, data protection violations, etc. One of the key points to make these services trustworthy—as required by PSD2—is to deploy an appropriate identity management solution. Among other identity management solutions, OAuth 2.0 (OAuth) and OpenID Connect (OIDC) are two widely used [Sim, LM20]. PSD2 states where personal data is processed—as in the authorization and authentication process—relevant security requirements laid down in Directive 95/46/EC should be met. The Directive is replaced with the GDPR.

OAuth/OIDC solutions [LM20, SB12] provide a secure and frictionless process. However, wrong implementation choices of these solutions may result in data breaches that impact the rights and freedoms of the large scale of personal data and data subjects [SCRS19]. A recent example is the internet bank account takeover of +1M users without user interaction due to an implementation flaw within their OAuth solution [Kre]. GDPR requires conducting a DPIA when data processing is likely to result in high risks to the rights and freedoms of the data subject. In particular, when the processing involves a large amount of personal data and affects a large number of data subjects [Arta]. That is the case for the authorization and authentication process.

Conducting a DPIA-compliant risk assessment for OAuth/OIDC-based solutions re-

¹The work is published in [DSCR21]

quires to:

- assess the risk for both IdMP's deployment and its integration within web applications (hereafter clients);
- face a maze of documents and guidelines to perform a comprehensive and flawless risk assessment which is a challenging task for non-security experts;
- be aware of security and privacy requirements of the client in question;
- be aware of DPIA requirements to conduct a risk analysis.

Meeting such requirements is a daunting task whose burden on the shoulder of controllers. To assist them, we adapted our methodology to conduct a DPIA-compliant risk analysis for OAuth/OIDC-based solutions. Our methodology is designed to address the requirements of OAuth/OIDC-based financial services and any OAuth/OIDC-based client processing either a special category of personal data or common personal data. Our main contributions are:

1. demystifying the maze of OAuth/OIDC documents to create a reference model that characterizes: (i) secure IdMPs deployment and integration, and (ii) privacy-preserving components to meet DPIA requirements;
2. formalizing a trade-off DPIA-compliance risk analysis as an optimization problem, using the introduced reference model;
3. proposing a tool-supported methodology to solve the optimization problem and assist controllers in evaluating and modeling risks;
4. analyzing 19 well-known IdMPs for their compliance with OAuth/OIDC security-related recommendation;
5. suggesting appropriate IdMP, from the well-known IdMP, to controller based on their operating domain;
6. warning when either the employed IdMP or its implementation does not comply with the required security and privacy level.

Structure of the Chapter. Section 6.1 provides some basic knowledge about the OAuth and OIDC protocols. Section 6.2 discusses the importance of the risk analysis for OAuth/OIDC solutions and re-identifies the two problems in the context of OAuth/OIDC solutions. While, Section 6.3 elaborates on the methodology to solve the problems. Section 6.4 discusses the related works, and Section 6.5 concludes the chapter.

6.1 Background

6.1.1 Access Delegation: OAuth Standard

OAuth [Har12] is an authorization protocol that provides a mechanism for resource owners to delegate application access to their information hosted in a resource server without giving their credentials (user name and password). In simple words, the application redirects the resource owners through the browser into the IdMP authorization server, where the resource owners consent and perform the authentication. After the successful authentication of resource owners, the authorization server issues an `access_token` that the application uses to access the resource owners' resources in the resource server.

To release an `access_token` to client for granting access to a resource, the OAuth WG defines four grant types *RO Password Credentials*, *Implicit*, *Authorization Code*, and *Client Credentials*. They must be picked according to the involved entities and the scenario. They differ in the process of obtaining tokens. *Client Credentials Flow* is suitable when the authorization is limited to resources under the control of client (e.g., during server to server communication). *RO Password Credential Flow* is suitable when there is a high-level trust establishment between resource owner and client. *Implicit Flow* is optimized for user agent based (i.e., web browser) applications which are developed using a scripting language. *Authorization Code Flow* is the most used popular grant type that provides a few important security benefits:

- it provides a mechanism to authenticate application at the authorization server;
- it transmits the `access_token` directly to the third-party application without passing it through the browser; and
- it avoids exposing of the `access_token` into intermediary entities, including the resource owners.

The OAuth working group have published a new OAuth Standard called OAuth 2.1 [HPL12] which mandates the following two grant types: *Authorization Code*, and *Client Credentials*.

6.1.2 Single Sign On: OpenID Connect Standard

OpenID Connect (OIDC) is an authentication layer developed on top of the OAuth standard. OIDC adds two main features into the OAuth standard: the `id_token` and

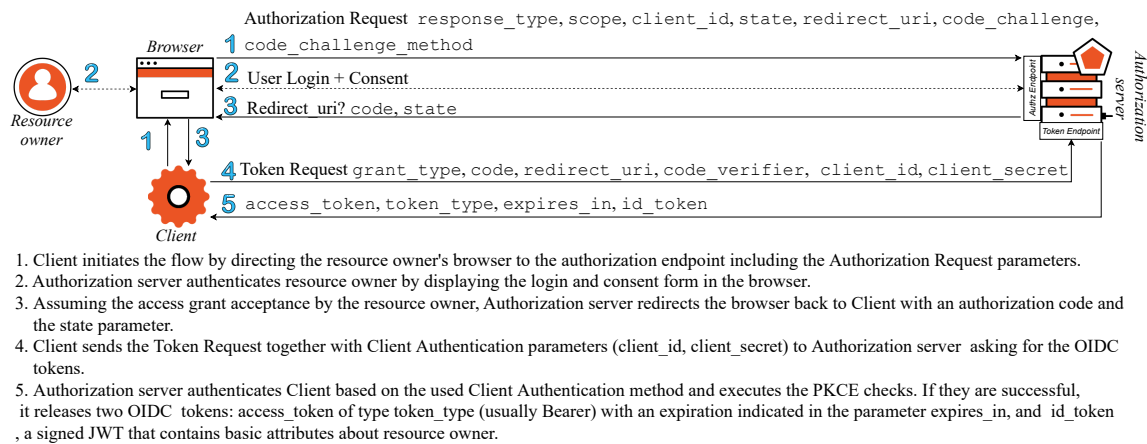


Figure 6.1: OAuth 2.0 Authorization Code Flow with Code Challenge.

the *userInfo* endpoint. The `id_token` is a structured JSON token [JBS15] that contains information about the token issuer (the OAuth provider), the subject (user identifier) and the audience (the intended application), all signed by the OAuth provider. This token enables the application to verify that the received token is issued for its previous token request. The *userInfo* endpoint is used to obtain identity-related attributes (e.g., the email and address). The *Authorization Code* flow with the Proof Key for Code Exchange (PKCE), prescribed in [SBA15] and illustrated in Figure 6.1, encompasses the following steps:

- the application sends the authentication request to the IdMP. This request contains the OAuth parameter (`client_id`, `redirect_uri`) together with the so-called PKCE parameters, namely the code challenge (`code_verifier`) and the code challenge method `t_m`;
- the IdMP's authorization server authenticates the resource owners and establishes whether the resource owners has granted or denied the access request;
- Assuming successfully authentication and the access grant acceptance by the resource owners, authorization server redirects browser back to application with an Authorization code.
- application sends the Authorization code, PKCE code verifier and the related *client authentication* method parameters (e.g., `client_secret`);
- authorization server computes the code challenge value using `t_m` and code verifier and compares it with the `t` value (the code verifier) received in Step 1. If they are the same, it releases an `access_token` and `id_token` to application.

Table 6.1 lists query parameters of the authorization and token request for the OIDC flow with *PKCE*.

Table 6.1: OIDC query parameters of Authorization Code Flow With Code Challenge.

Tag	Query Parameter	Value	Description
<i>OIDC_A</i>	response_type	code	Determines the authorization flow to be used.
	scope	oidc	A space-separated string of the scopes being requested and the <i>oidc</i> must be present when <i>OIDC</i> is supported .
	client_id	string	The unique identifier of the app.
	state	string	A random string generated by the app used for maintaining state between the request and the callback.
	redirect_uri	string	The URL to return to after the successful authentication.
<i>PKCE_A</i>	code_challenge	string	A string generated by applying <i>code_challenge_method</i> to the <i>code_verifier</i> value.
	code_challenge_method	plain or s256	Transformation method used to calculate <i>code_challenge</i> .
<i>OIDC_T</i>	grant_type	authorization_code	Determines the way <i>C</i> gets the <i>OIDC-Core</i> tokens.
	code	string	The authorization code received in Step 3 from <i>AS</i> .
	redirect_uri	string	The URL used in Step 1
<i>PKCE_T</i>	code_verifier	string	A high-entropy cryptographic random string
<i>ClientAuthentication</i>	client_id	string	The unique identifier of the app.
	Client_secret	string	The unique credential of the app.

6.2 Problem Definition and OAuth/OIDC Reference Model

Analyzing risks to the rights and freedoms of data subjects is an important step of a DPIA [Cla09, SWB⁺12, OSG⁺11, Artc, CNI12a], and it is critical but complex for OAuth/OIDC solution. That is due to:

1. many choices of IdMPs with various configuration options;

2. various implementation patterns;
3. many security implications and guidelines documents;
4. lack of guidelines to meet privacy goals, using OAuth/OIDC components.

Therefore, we adapted our methodology to perform a DPIA-compliant risk analysis that requires an appropriate level of security and privacy protection according to the client's baseline in question. Therefore, As such, we identify the following two problems:

P_{risk} OAuth.OIDC security and privacy risk assessment and trade-off analysis, taking into account the risk propagation.

$P_{compliance}$ compliance assessment w.r.t. security and privacy-related BCPs.

Before elaborating on the problems and our methodology, we introduce a reference model of OAuth/OIDC solutions (Section 6.2.1), extracted from the various OAuth/OIDC security and privacy-related documents (Section 6.2.2). In Section 6.2.3, we formalize the two above-mentioned problems. Note that, the identified problems and notations in this section are customized version of the ones introduced in Chapter 2.

6.2.1 OAuth/OIDC Reference Model

To build the reference model, we studied OAuth/OIDC security documents (e.g., [Har12, SBJ⁺14]) to extract the components that protect OAuth/OIDC deployment to satisfy privacy and security goals (introduced in Section 4.3). We call these components *atomic features* (*af*).

The focus of the reference model is on the features that the protocols offer, however it can extended to support deployment specific features.

Table 6.2 represents the reference model. The second column of the Table lists the *afs*. They are named after either:

- parameter name (e.g., nonce);
- parameter value (e.g., code);
- functionality aspects (e.g., full redirect_uri); or

Table 6.2: OAuth/OIDC Reference Model

Deployment place	Atomic features	Threat (T)	Goal (G)	Consecutive T	Consecutive G	PL	LL
Security Feature							
Authorization request	code	Obtain AT	PD Conf	-	-	3	3
	token					1	
	client_credentials					3	
	password					1	
	hybrid					3	
	nonce	Obtain AT , Session misuse	PD Conf	-	-	5	5
	state	Session misuse	PD Conf	-	-	5	5
	request	Obtain code	AT Conf	Obtain AT	PD Conf	5	5
	request_uri					5	
	query					1	
	form_post	Obtain code	AT Conf	Obtain AT	PD Conf	5	5
	fragment					1	
	query	Obtain AT , Session misuse	PD Conf	-	-	1	5
	Code challenge					5	
	plain	Obtain AT , Session misuse	PD Conf	-	-	1	5
	s256					5	
Token request	mtls	Obtain AT	PD Conf	-	-	3	3
	client_secret_jwt					3	
	private_key_jwt					3	
	client_secret_basic					2	
	cleint_secret_post					2	
	code_verifier	Obtain AT , Session misuse	PD Conf	-	-	5	5
Authorization request / Token request	full redirect_uri ^{idmp}	Obtain code	AT Conf	Obtain AT	PD Conf	3	3
	pattern redirect_uri ^{idmp}					1	
Header	binding IdMP metadata ^{cl}	Obtain AT	PD Conf	-	-	2	2
	referrer ^{cl}	Obtain code	AT Conf	Obtain AT	PD Conf	3	3
Console	distinct redirect_uri ^{cl}	Obtain code	AT Conf	Obtain AT	PD Conf	5	5
Client check	open redirect validation ^{cl}	Obtain code	AT Conf	Obtain AT	PD Conf	5	5
	state validation ^{cl}	Obtain code	PD Conf	-	-	5	5
	storing IdMP metadata ^{cl}	Obtain code	AT Conf	Obtain AT	PD Conf	5	5
	issuer validation ^{cl}	Obtain code	AT Conf	Obtain AT	PD Conf	5	5
	id token validation ^{cl}	Impersonation	PD Conf	-	-	5	5
Privacy Features							
Authorization request	claims	Comp data mini	Data mini			5	5
	scope	Comp data mini	Data mini			5	5
	purpose	Comp. Pur spec, Trans	Pur Spec, Trans			5	5
	verified_claims	Comp. PD accuracy	PD accuracy			5	
	vot	Impersonation, Comp PD accuracy	PD accu, PD Conf			5	5
	acr					5	
	login	Comp transparency	Transparency	-	-	3	3
	select account					3	
	consent					3	
	pairwise ^d	Linkability	Unlinkability	-	-	5	5
Console	public ^d					1	

LEGEND. idmp: idmp only feature, cl: client only feature, comp: compromise, PD: personal data, AT: access token, trans: transparency
data mini: data minimization, conf: confidentiality, pur spec: purpose specification, PL: protection level, LL: likelihood level

- client specific implementation-related tasks (e.g., Id token validation);

and are to be set/implemented either in:

- authorization/Token requests;

- IdMP developer console, set by controllers;
- the Header; or
- are checks implemented by the controller.

Column *Deployment Place* in Table 6.2 represents where each *af* need to be set/implemented. For example, the controller needs to set *subject identifier type*² that could be either pairwise or public, in the IdMP developer console. Appendix D.1 describes each feature.

The OAuth Working Group and the OpenID Foundation recommends different *afs* for different scenarios—with different level of contributions (*protection level*)—to achieve a common goal. We group together such *afs*, and call them *composed feature* (*cf*). A client can implement one *af* from a *cf* per request. For example, request, request_uri and query are grouped together under *cf Request*. They are introduced to meet goal *access token confidentiality*, by protecting authorization request against the threat *obtain code* (see Table 6.2). While *af request* and *request_uri* pass OAuth/OIDC requests in a signed and optionally encrypted single, self-contained parameter manner to preserve integrity and confidentiality; *af query* passes it directly in the URL. Thus, the first two provide a higher protection level. Accordingly, the protection level for the discussed *afs* are 5, 5, and 1, respectively.

Table 6.3: Composed Features.

Composed Feature	Related Atomic Features
Response type	{code,token,client_credentials,password,hybrid}
Request	{request,request_uri,query}
Response mode	{form_post,fragment,query}
Code challenge method	{plain,SHA256}
Client authentication	{mTLS,client_secret_jwt,private_key_jwt,client_secret_basic,client_secret_post}
Redirect uri	{full redirect_uri,pattern redirect_uri}
Identity proofing	{vot,acr}
Prompt	{login,select_account,consent}
Subject type	{public,pairwise}

This is an important consideration, as it allows controllers to make an informed decision on the IdMP s/he chooses (not all IdMPs support all the *afs*), or/and the *afs* they decide to implement. The seventh column of the Table 6.2 lists the calculated Protection Level (PL). The likelihood level for each *af* is the same level as its PL. Because, when an *af* with protection level *X* is supported/implemented, it means that the *af* can contribute to decrease the likelihood of a given threat to *X*. Thus, if

²A locally unique and non-reassignable identifier within the Issuer for the End-User, to be consumed by the Client

it is not then the system dose not have that reduction of likelihood level. In case of *cfs*, the likelihood level is assigned to the *cf*. That is because the related threat(s) only happen if the controller does not impalement no *afs* of a *cf*. The sixth column of Table 6.2 lists the calculated Likelihood Level (LL). Protection/likelihood levels range from 1 to 5. Controllers can modify the likelihood and protection level if needed. Note that the calculation of likelihood and protection level in this context is unlike the main methodology, where we calculate them based on the number of implemented/overlooked security control or privacy tactics.

Each *af/cf* is introduced to protect OAuth/OIDC deployment against a threat to satisfy privacy/security goals. A threat could expose the system to another threat, which itself compromises another goal. We call them *consecutive threats* and *consecutive goal*. They are as likely to raise as their main threat. For example, as represented in Table 6.2, not implementing *af* request leads to threat *obtain code*, which itself let the attacker to *obtain access token*. They relate to goal *access token confidentiality*, and *personal data confidentiality*, respectively.

Note that, for the sake of simplicity Table 6.2 only has considered the response type code flow. The complete Table which lists related information for all the response type, namely code, token, hybrid, client credential and password, can be found in Appendix D.2.

6.2.2 Best Current Practice Specification

Best Current Practices (BCPs) are defined as a proper mechanism for minimizing the impact of attacks on applications. They present a reliable and tested solution to deal with recurring security threats [OMGMR⁺10, FKS16, FKS17, Hof19]. They provide specific recommendations and easy to implement mitigations for both IdMPs and controllers that aim to avoid being attacked through implementation flaws and known anti-patterns; and give additional protection to scenarios that demand a higher level of security, such as Fintech.

In this work, we have extracted two BCPs: (i) *OAuth/OIDC security BCPs* (See Section 6.2.2.1); and (ii) *OAuth/OIDC privacy BCPs* (See Section 6.2.2.2). While OAuth/OIDC security BCPs are extracted from the OAuth/OIDC documentations, OAuth/OIDC privacy BCPs are our recommendations to meet the privacy goals to satisfy DPIA requirements.

Then, we suggest two *authorization* and *token requests* schemas, considering the introduced BCPs, to ensure that the requests comply with the DPIA requirements (See Section 6.2.2.3).

6.2.2.1 OAuth/OIDC Security BCPs

The security goal of identity management is to protect the *confidentiality of token* and, consequently, the *confidentiality of personal data*. The level of protection that a client requires, depends on the type of data involved, e.g., accessing online banking or online health services requires a more robust authentication process. Therefore, we consider two categories of security BCPs:

- *OAuth/OIDC Security BCP*: for when a minimum level of security is appropriate, that is, when the baseline is set to *low*. For example, OAuth/OIDC BCPs recommend *afs* `client_secret_basic` or `client_secret_post` to authenticate client. They satisfy a minimum level of protection against *obtain access token* threat.
- *FAPI Security BCP*: for when a higher level of security is required; like when financial data are involved. As such, we apply FAPI BCPs not only for financial services but when the baseline is either *high* or *moderate*. For example, unlike OAuth/OIDC, to authenticate clients FAPI BCPs recommend *afs* `client_secret_jwt`, `private_key_jwt`, or `mTLS` as they provide higher level of protection against *obtain access token* threat.

We have extracted the OAuth/OIDC security BCPs from OAuth Authorization Framework [Har12], OpenID Connect Core [SBJ⁺14], OAuth Threat Model and Security Consideration [LMH13] and OAuth Security BCPs [LBLE20]. For defining the FAPI BCPs, we have considered the FAPI Baseline Security Profile (part1) [SBJ]. Table 6.4 lists FAPI BCPs and OAuth/OIDC BCPs.

6.2.2.2 Our Recommended OAuth/OIDC Privacy BCPs

Neither OAuth/OIDC BCPs nor FAPI BCPs provide specific recommendations to meet privacy goals (See Section 4.3). However, to comply with the DPIA requirements, controllers need to address privacy goals. To achieve them, we use OAuth/OIDC optional *afs* and the ones introduced in the following documents: OIDC iGov Profile [ID18], OIDC for Identity Assurance [TD], and Vector of Trust [RJ18]. Table 6.5 lists the *afs* and the privacy goal they address. Bellow, we detail how the selected *afs* can help addressing the privacy goals.

Confidentiality and Data Accuracy. Composed feature *Identity proofing* is to request IdMP to guarantee a certain level of identity proofing, that comprises of *afs* `acr_value` and *Vector of Trust* (`vot`) [RJ18]. Since `vot` conveys trust informa-

Table 6.4: Security BCPs for FAPI and OAuth/OIDC Security.

Composed Feature	FAPI Security BCP	OAuth/OIDC Security BCP
Response type	authorization_code	authorization_code or client_credential
Client authentication	mTLS or client_secret_jwt or private_key_jwt	client_secret_basic or client_secret_post
Code challenge method	S256	S256
Request	request or request_uri	-
Redirect uri	full_redirect_uri	full_redirect_uri
Prompt	consent	consent
Response mode	Form_post	Form_post
Identity proofing	[P3. Ac. Ce. Mc] or acr_level 2/3	[P2. Ac. Cd. Mb] or acr_level2
Subject type	pairwise	pairwise
Atomic features	state	state
	nonce	nonce
	claims	claims
	purpose	purpose
	verified claims	verified claims
	iss_validation	iss_validation
	acr_level2 or higher	acr_level2
	id_token_validation	id_token_validation
	no-referrer	no-referrer
	distinct_redirect_uri	distinct_redirect_uri
	open_redirect_validation	open_redirect_validation
	state_validation	state_validation
	binding_IdP_metadata	binding_IdP_metadata
	storing_IdP_metadata	storing_IdP_metadata

tion with more actionable data and expressiveness, we recommend to use it over `acr_value`. It defines four orthogonal components, as follows:

1. identity proofing (P): to assess how strongly the IdMP has verified the attributes that data subject had provided to authenticate. This component has values ranging from P0 to P3. For example, P1 means that data subjects' attributes are self-asserted, while P2 means that their attributes have been proofed either in person or remotely using a trusted mechanism (e.g., social proofing). Needless to say that higher level values satisfy the lower level data accuracy requirements. Only one distinct value from this category must be used within OAuth/OIDC solutions;
2. primary credential assurance (C): to assess how strongly IdMP has verified the means data subject used to authenticate. In simple words, it represents how easily the data subject credentials could be spoofed or stolen. This component defines values from C0, Ca to Cg. For example, Cc represents the usage of shared secret (e.g., username and password combination), while Cd represents cryptographic proof of key possession using shared key. Multiple values from this category may be used within OAuth/OIDC solutions;
3. primary credential management (M): to convey information about the expected life cycle of means data subject used to authenticate. In particular, it verifies

the strength of policies, practices, and security controls used in managing the credentials at the IdMP and its binding to the intended data subject. This component has values from Ma to Mc. For example, Ma means that the data subject chooses its own credentials and must rotate and revoke them manually. Multiple values from this category may be used in OAuth/OIDC solutions; and

4. assertion presentation (A): to assess how well the digital identity can be communicated across the network without information leaking to unintended parties and without spoofing. This component has values from Aa to Ad. For example, Ab requires that the assertions provided by IdMP is signed and verifiable. In addition, they passed through the user agent.

We suggest using *[P2.Ac.Cd.Mb]* when common personal data are involved, and *[P3.Ac.Ce.Mc]* when special categories of data are involved. *[P2.Ac.Cd.Mb]* requires:

- to prove the identity either in person or remotely using a trusted mechanism to provides a stringent proofing that the digital identity corresponds to a real data subject (P2);
- the signed and verifiable assertion to be passed through a back channel which is more secure than passing through the user agent, and less probable to leak assertions to unintended parties or get spoofed (Ac);
- cryptographic proof of key possession using the shared key for primary credential usage, so it is hard to get spoofed by the adversaries (Cd);
- remote data subject credentials issuance and rotation/use of backup recovery (e.g., email verification), to enforce basic policies and security controls in managing the credential at the IdMP and its binding to the intended data subject (Mb).

While, *[P3.Ac.Ce.Mc]* requires:

- a binding relationship between the identity provider and the identified party (P3);
- the signed and verifiable assertion to be passed through a back channel which is more secure rather than passing through the user agent (Ac);
- cryptographic proof of key possession using an asymmetric key (Ce)
- proofing for data subject credentials issuance and rotation/revocation on suspicious activities to enforce stronger policies and security controls in managing the credential at the IdMP and its binding to the intended data subject (Mc).

Transparency. To prompt data subject for re-authentication and collect their consent before returning information from IdMP, feature *prompt* need to be set to *consent*. Data subjects also need to be informed about the purpose of the processing which we address below.

Accuracy, Purpose Specification, and (more) Transparency. The *Identity Assurance* profile [TD] defines a generic mechanism through defining a new parameter called `verified_claim` to provide controllers with a set of claims about end-users (e.g., name, and address) and the respective metadata and verification evidence to verify them. This way, controllers cannot mix up verified and unverified claims. The `verified_claims` is an object or array containing one or more verified claims objects. Following, we define the `verified_claims` objects and then we explain how they help addressing the mentioned privacy goals:

- *verification*. To represents an object that provides information about the verification process. The verification can consist of optional and mandatory parameters, such as `trust_framework` (mandatory), `time` (optional), and `evidence` (optional).
 - `trust_framework` defines the identity verification process and the identity assurance level of the IdMP. An example value is *eidas_ial_high* that provide a "High" level of assurance. *eIDAS* (electronic IDentification, Authentication and trust Services) is an EU regulation on electronic identification and trust services for electronic transactions in the European Single Market [eID14].
 - `time` represents the date and time when the identity verification process took place, and `evidence` is a JSON array that provides information concerning the evidence used by the identity provider to verify the end-user's identity.
 - `evidence` contains information about the evidence that the IdMP use to verify the user's identity. It defines the following types of evidence: `id document`, `utility bill`, and `qes` (verification based on an eIDAS Qualified Electronic Signature).
- *claims*. To represent the claims about the end-user which are verified in accordance with the policies determined by the corresponding verification element. The `claims` element can contains the standard end-users claims as defined in the OIDC [SBJ⁺14] document (e.g., name) and the new end-users claims that are defined in the *Identity Assurance* [TD] document (e.g., `place_of_birth`). The *Identity Assurance* introduces an additional field `purpose` to allow controller state the purpose for obtaining certain user claim from the IdMP.

As such, the profile enables controllers to achieve the following privacy goals:

1. *accuracy*: by using *evident* to ask for the trust framework governing the identity verification, the identity assurance level of the IdMP, and the evidence used to verify the user’s identity; and by using *time* to ask for the date and time when the IdMP has verified the identity. We also suggest using the claim *updated_at*, which is one of the standard claims introduced in OIDC core [SBJ⁺14]. As the claim allows to check when the user information was last updated;
2. *purpose specification*: by using field *purpose* to enable controllers to state the purpose of asking each individual claim;
3. *Transparency*: as the IdMP MUST display the specified purpose in the respective user consent screen(s).

Table 6.5: Privacy BCPs.

Privacy BCPs	Goal
claims	Personal Data Minimization
scope	Personal Data Minimization
purpose	Purpose Spec
verified claims	Personal Data accuracy, Integrity
vot:[P3.Ac.Cc.Mc]/Higher	Personal Data accuracy
acr: acr_level2/3	Personal Data Confidentiality
consent	Transparency
pairwise	Unlinkability

Data Minimization. OIDC core suggests minimizing the amount of information requested from the EU. *af* claims enables controller to ask for specific EU claims. Note that *acr_values* also limits the data based on the requested level of assurance.

Data Unlinkability. OIDC introduces two types of subject identifier, namely: *public* and *pairwise*. The former assigns an identifier to an EU within different controllers, while the latter provides one unique end user’s identifier per controller. To fulfill this goal, the controller needs to use *pairwise* identifiers.

Unaddressed Goals and GDPR Data Protection Principles. OIDC states that “the end-user will be given the option to have IdMP decline to provide some or all information requested by controllers [SBJ⁺14]”, that is privacy goal *Interveinability*. While, privacy goal *Accountability* requires the controller to place appropriate technical and organizational measures and demonstrate its effectiveness when requested. Such measures include adequate documentation on data processing. Meeting the two mentioned goals depends on IdMP implementation, and the controller has no control over it.

Another unaddressed goal is *Storage Limitation principle*, which requires controllers to store personal data no longer than necessary (article 5.1.e of the GDPR). OAuth/OIDC solutions do not provide such measures.

```

1 {
2   "client_id": "value",
3   "request": "jwt value"
4 }
5 // JWT Value:
6 "redirect_uri": "value",
7 "scope": "openid",
8 "response_type": "code",
9 "nonce": "value",
10 "state": "value",
11 "response_mode": "form_post",
12 "code_challenge": "value",
13 "code_challenge_method": "S256",
14 "claims": {
15   "userinfo": {
16     "verified_claims": {
17       "verification": {
18         "trust_framework": "value",
19         "time": { "max_age": "value" }
20       },
21       "evidence": [
22         { "type": { "value": "value" } }
23       ]
24     },
25     "claims": {
26       "name of claim": {
27         "essential": true,
28         "purpose": "Specify the purpose"
29       },
30       "update_at": {
31         "essential": true
32       }
33     }
34   }
35 },
36 "prompt": "consent login",
37 "vot"/"acr_values": "value"
38 }- vot value: "P3.Ac.Ce.Mc" / acr value: "LoA2" or higher

```

(a) Authorization Request: High and Moderate Baseline

```

1 {
2   "client_id": "value",
3   "redirect_uri": "value",
4   "scope": "openid",
5   "response_type": "code",
6   "nonce": "value",
7   "state": "value",
8   "response_mode": "form_post",
9   "code_challenge": "value",
10  "code_challenge_method": "S256",
11  "claims": {
12    "userinfo": {
13      "verified_claims": {
14        "verification": {
15          "trust_framework": "value",
16          "time": { "max_age": "value" }
17        },
18        "evidence": [
19          { "type": { "value": "value" } }
20        ]
21      },
22      "claims": {
23        "name of claim": {
24          "essential": true,
25          "purpose": "Specify the purpose"
26        },
27        "update_at": {
28          "essential": true
29        }
30      }
31    }
32  },
33  "prompt": "consent login",
34  "vot"/"acr_values": "value"
35 }- vot value: "P2.Ac.Cd.Mb" / acr value: "LoA2"

```

(b) Authorization Request: Low Baseline

```

1 { // Client Secret JWT & Private key JWT client authentication
2   "grant_type": "authorization_code",
3   "code": "value",
4   "redirect_uri": "value",
5   "code_verifier": SHA(code_challenge)
6 }
7 "client_id": "value",
8 "client_assertion_type": "urn:ietf:params:oauth:client-assertion-type:jwt-bearer",
9 "client_assertion": {client assertion}
10 }
11 // client assertion
12 {
13   "iss": "value", // issuer of the JWT
14   "sub": "value", // data subject
15   "aud": "value", // audience, can be the authorization server token endpoint URL.
16   "exp": "value",
17   "nbf": "value",
18   "iat": "value",
19   "jti": "value" // JWT id
20 }
21 // mTLS Client authentication
22 {
23   "grant_type": "authorization_code",
24   "code": "value",
25   "redirect_uri": "value",
26   "client_id": "value",
27   "code_verifier": SHA(code_challenge)
28 }

```

(c) Token Request: High and Moderate Baseline

```

1 { // Client authentication type: client_secret_post
2   "grant_type": "authorization_code",
3   "code": "value",
4   "redirect_uri": "value",
5   "client_id": "value",
6   "client_secret": "value",
7   "code_verifier": SHA(code_challenge)
8 }
9 // Client authentication type: client_secret_basic
10 {
11   "grant_type": "authorization_code",
12   "code": "value",
13   "redirect_uri": "value",
14   "authorization": BASE64-ENCODE("client_id", "client_secret"),
15   "code_verifier": SHA(code_challenge)
16 }

```

(d) Token Request: Low Baseline

Figure 6.2: BCPs-Compliant Request Schema

6.2.2.3 BCP-Compliant Authorization/Token Request Schemas

Considering the reported security/privacy BCPs, we have generated two *authorization* and *token requests* schemas to ensure that the requests comply with the DPIA requirements. We considered *OAuth/OIDC Security BCP* when common personal data are involved, and *FAPI Security BCP* when special category of personal data is involved. Both schemas are compliant with BCPs OAuth/OIDC Privacy because the privacy goals shall be met either way.

Figure 6.2 represent BCP-Compliant authorization and token requests. The *afs* indicated with an asterisk are the optional features and the ones highlighted in blue are the features that are taken from OIDC for Identity Assurance [TD] and Vector of Trust [RJ18]. We use the claim *updated_at* as an essential claim to check whether the claims are updated. The other claims that the controller needs to ask, we suggest them to be only necessary ones for the identified purpose.

6.2.3 Problem Definition

In this section we formalise the problems, namely P_{risk} and $P_{compliance}$, considering the OAuth/OIDC reference model reported in Table 6.2.

Let $\mathcal{AF}$ be the set of *afs* associated with an OAuth/OIDC deployment shown in the second column of Table 6.2. We split the set $\mathcal{AF}$ in three disjoint subsets: $\mathcal{AF} = \mathcal{AF}_{common} \cup \mathcal{AF}_{idmp} \cup \mathcal{AF}_{cl}$.

The set $\mathcal{AF}_{common}$ includes the *afs* that the client cannot implement unless the IdMP supports them, like *nonce*. An IdMP can support more than one *af* from a *cf*, while the client can implement only one for a given request. The set $\mathcal{AF}_{idmp}$ includes *afs* that IdMPs need to enforce (marked with the “idmp” superscript in Table 6.2); clients need only to adopt them, like *pattern_redirect_uri*. The set $\mathcal{AF}_{cl}$ includes the *afs* that clients need to implement and checks that they need to perform (marked with the “cl” superscript in Table 6.2), like *issuer validation*. Let $support_{idmp}$ be a Boolean mapping from the set $\mathcal{AF}_{common} \cup \mathcal{AF}_{idmp}$ for *idmp* ranging over a given set of IdMPs. An atomic feature *af* maps to a true value iff *idmp* supports *af*. Similarly, let $implement_{cl}$ be a Boolean mapping from the set $\mathcal{AF}_{common} \cup \mathcal{AF}_{cl}$ for a given client *cl*. An atomic feature *af* maps to a true value iff *cl* implements *af*.

Notice that, for $af \in \mathcal{AF}_{common}$, we say that $implement_{cl}$ is *constrained* by $support_{idmp}$, meaning that $implement_{cl}$ is strictly dependent on $support_{idmp}$, i.e. $af \in \mathcal{AF}_{common}$ can map to true only if it maps to true in $support_{idmp}$. Indeed, the entity responsible to implement the client can decide to implement or not some atomic features among the one supported by *idmp*, but in any case it cannot implement the atomic features

that are not supported by *idmp*.

Problem P_{risk} definition. Let $\mathcal{CF}^* \subset \mathbf{P}(\mathcal{AF})$ (where $\mathbf{P}$ stands for the power set) be a set of sets of *afs*, including the *cfs* defined in Table 6.3 as well as a set $\{af\}$ for each atomic feature $af \in \mathcal{AF}$ that does not belong to any composed feature in Table 6.3. Thus, $\mathcal{CF}^* = \{\dots, \{\text{nonce}\}, \{\text{state}\}, \{\text{request}, \text{request_uri}, \text{query}\}, \dots\}$. Note that all the sets $S \in \mathcal{CF}^*$ are pairwise disjoint and $\bigcup_{S \in \mathcal{CF}^*} S = \mathcal{AF}$, that is $\mathcal{CF}^*$ is a partition of $\mathcal{AF}$. Let $\mathcal{T}$ be the set of threats and consecutive threats, listed in columns 3 and 5 of Table 6.2. Let $\mathcal{G}$ be the set of goals and consecutive goals, listed in columns 4 and 6 of Table 6.2. We thus define the following mappings and relations:

- let p be a mapping from $\mathcal{AF}$ to the set $\{1, \dots, 5\}$ of protection levels. The definition of this mapping can be obtained by considering the features in column 2 and the corresponding protection level in column 7 of Table 6.2.
- let the likelihood mapping ℓ be a mapping from $\mathcal{CF}^*$ to the set $\{1, \dots, 5\}$ of likelihood levels. The definition of this mapping can be obtained by considering the (sets of) atomic features in column 2 and the corresponding likelihood level in column 8 of Table 6.2.
- let $CF2T \subseteq \mathcal{CF}^* \times \mathcal{T}$ be a relation between each composed feature $cf \in \mathcal{CF}^*$ and its related threat. The pairs in this relation can be defined by reading the elements reported in columns 2 and 3 of Table 6.2. In the rest of this paper, we also use the notation $T(cf)$ to indicate the set of threats related to a composed feature cf .
- let $T2G \subseteq \mathcal{T} \times \mathcal{G}$ be a relation between each threat and the goal compromised by the threat itself. The pairs in this relation can be defined by reading the elements reported both in columns 3 and 4, and 5 and 6 of Table 6.2. Indeed, the relation between a threat and the goal is independent of the fact that the threat is consecutive or not of another threat. We also use the notation $g(t)$ to indicate the goal related to a threat $t \in \mathcal{T}$.
- let $T2CT \subseteq \mathcal{T} \times \mathcal{T}$ be a relation between a threat and its consecutive threat. The pairs in this relation can be defined by reading the elements reported in columns 3 and 5 of Table 6.2. We also use the notation $CT(t)$ to indicate the set of threats consecutive to the threat t , and $CT(\mathcal{T}) \triangleq \bigcup_{t \in \mathcal{T}} (CT(t))$.

The problem P_{risk} consists in finding the *idmp* and mapping $implement_{cl}$ such that

$$\min_{idmp, implement_{cl}} \mathcal{R}(p, \ell, support_{idmp}, implement_{cl}, CF2T, T2G, T2CT) \quad (6.1)$$

subject to $idmp \in IdMPs$ and $cl \in ClAdm$, where $IdMPs$ is a set of IdMPs that support certain features and $ClAdm$ is the set of admissible mappings for a given client.

The set $IdMPs$ and the admissible mappings $ClAdm$ come from external considerations performed by the controller of the client. For instance, IdMPs can be affected by the costs of identity providers' services or which kind of features they support. Similarly, the controller can consider that some features—among the ones constrained (as defined above) by the selected $idmp$ —will take longer to implement or charge more in terms of costs. Thus, the controller can further constrain the admissible $implement_{cl}$ mappings accordingly.

$\mathcal{R}$ is thus an operator that returns the risk level given the selected $idmp$, the configuration of the client cl , and the protection and likelihood mappings. In our case, $\mathcal{R}$ is instantiated with the procedure supported by the RiskML tool. First, this allows the controller to perform a risk assessment taking into account the risk propagation, namely the propagation of the negative effects of the threats and the positive effects of the mitigation offered by implementing the (security measures corresponding to the) selected propositions. Second, RiskML support a trade-off analysis, allowing the controller to consider the risk associated with each choice.

As a final remark, note that the problem P_{risk} is solved by the formula (6.1) considering $p, l, CF2T, T2G$, and $T2CT$ constant (obtained from Table 6.2), while $support_{idmp}$ and $implement_{cl}$ can change. Therefore, the problem is decidable because it can be expressed as a combinatorial optimization problem with many finite possibilities depending on the number of considered $IdMPs$ and on the cardinality of the considered atomic features in $\mathcal{AF}$: all the possibilities can be enumerated, the corresponding risk evaluated and the minimum value selected.

Problem $P_{compliance}$ definition. Let us define a complex proposition as a formula obtained from afs in $\mathcal{AF}$ and logical connectives. Let us call $BCPs_{FAPI}$ and $BCPs_{OAuth/OIDC\ Privacy}$ the set of complex propositions reported in the second column of Table 6.4 and Table 6.5, resp. Let us call $BCPs_{OAuth}$ the set of complex propositions obtained from $BCPs_{FAPI}$ by applying the changes mentioned in Section 6.2.2.

We thus specify the problem $P_{compliance}$ of compliance assessment w.r.t. security (OAuth BCPs and FAPI) and privacy-related BCP as follows: given the sets of complex propositions $BCPs_{OAuth}$, $BCPs_{FAPI}$, and $BCPs_{OAuth/OIDC\ Privacy}$, we state that an $idmp$ is compliant with the OAuth, FAPI, privacy-related BCPs, resp., whether the Boolean mapping $support_{idmp}$ satisfies all the complex propositions in $BCPs_{OAuth}$, $BCPs_{FAPI}$, and $BCPs_{OAuth/OIDC\ Privacy}$, resp. Similarly, we state that a deployment of a client cl is compliant with the OAuth, FAPI, privacy-related BCPs, resp., whether the Boolean mapping $implement_{cl}$ satisfies all the complex propositions in $BCPs_{OAuth}$, $BCPs_{FAPI}$, and

BCPs_{OAuth/OIDC Privacy}, resp.

6.3 Application of Our Methodology on OAuth/OIDC-based Solutions

This section discusses the adaption of our methodology to conduct a DPIA for OAuth/OIDC-based solutions. The first step of the methodology, namely *processing analysis*, comprises of two sub-steps; the first step is to learn about the organization as a whole and the second to learn about each data processing. In the context of identity solutions, some of these steps are not required as we focus only on protocol-related features and on the authentication/authorization process; we do not need to: draw MSC as data flow is standard; identify the duration of the process as it depends on life-time of the access token that is set by IdP; and identify supporting assets as we focus only on the features that these protocols offer and leave the proprietary solution that each IdP may offer. The second step of the methodology, namely *risk analysis*, comprises five sub-steps. The first two are to assess the implemented security and privacy controls, the third to check for vulnerabilities in supporting assets and controls, the fourth to check compliance of access control policies, and the last to generate a risk model. While the adapted version of the first two and the last sub-steps applies, the third and the fourth step are not required; as there are no supporting assets and security/privacy controls to check their vulnerabilities, and the controller can only read the data s/he asks.

Running Example. To illustrate the application of the methodology, we use a scenario that is inspired by the example provided in [Sak].

Graphy is a client that gets the users' financial data from their bank accounts and makes a graphical representation of their financial status. Users need to make a profile with the *Graphy*, and connect their bank accounts to it. *Graphy* utilizes OAuth/OIDC solutions to provide a smooth login and access delegation experience for its users.

6.3.1 Processing Analysis

The controller needs to identify the processor, data subject and data type category, estimate the impact level of processing, and the baseline.

Identifying Processor. In the context of OAuth/OIDC, client/app developer is controller and, IdMPs are processor. We provide three ways for controllers to identify the employed IdMPs: (i) we provide a list of popular IdMPs from which the controller can find the employed IdMPs, if not found, (ii) the controller can indicate the discovery endpoint URL of the employed IdMPs, or (iii) s/he can choose to reply to a questionnaire about the *afs* of IdMP. We elaborate on them in Section 6.3.2.1.

Identifying Data Subject and Data Type. To identify data subjects and data type, the controller needs to identify the economic sector (as discussed in Section 5.2.2). Data subject and data type categories are required to identify the impact level and the OAuth/OIDC-based service baseline in question.

Identifying Impact and Baseline. The impact and baseline are evaluated in the same way as the main methodology. In short, if any condition according to which a DPIA is required holds, the impact is *maximum*. If not, the impact is evaluated according to data type category involved, that is, *maximum* when special category of personal data, *significant* when personal data with high risks, and *moderate* when personal data are involved. The baseline will be set, accordingly. Please refer to Section 5.2.3, for the more detail. The baseline defines whether the controller needs to comply with OAuth/OIDC or FAPI BCPs (See Section 6.3.2.2).

Application of the step on the scenario. Graphy is the controller. The controller employs IBM for single sign-on (SSO) login—from the list of studied IdMPs—and allows users of Barclays bank for access delegation (AD) to link their bank accounts.

The service it provides belongs to *Activities auxiliary to financial services and insurance activities*. *Personal data and financial data of natural persons* are involved. The controller specified that a large scale of data subjects is using the service. as such the variable *impactValue* is set to 5 (maximum); and accordingly the *ProcessingBaseline* is set to *high*.

6.3.2 Risk Analysis

Having the necessary information to conduct a risk analysis, this section explains how we apply our methodology to answer the two identified problems in the context of the OAuth/OIDC-based methodology: P_{risk} and $P_{compliance}$

6.3.2.1 Addressing P_{risk}

This step aims to assess employed IdMPs and the implementation details with regards to their integration within the client. That is to identify any threat(s) they may pose to the rights and freedoms of data subjects. For that, we introduce the following two components: *IdMP Processor* and *Client Processor*. Each processor output a document: *IdMP Specification* and *Client Specification*, respectively. The documents will input into the RiskML to model and evaluate the risks. Below, we elaborate on the two processors and the application of them in the scenario. Then, we discuss the modeling and evaluation.

I. IdMP Processor The processor aims to assess which are the $afs \in \mathcal{AF}_{common} \cup \mathcal{AF}_{idmp}$ that the employed IdMPs support. More formally, the IdMP processor aims to specify the *support_idmp* Boolean mapping for the employed *idmp*.

In the first step, the controller has given three options to identify the employed IdMPs: (1) finding the employed IdMP from list of popular IdMPs, (2) indicating discovery endpoint URL, and (3) replying to a questionnaire. According to the taken option, the processor assesses the IdMP. Following, we elaborate on each option:

- opt 1. *finding it from the list of popular IdMPs*: we have studied popular IdMPs for their $\mathcal{AF}$ and stored their truth values in a database called *IdMP_DB*. Table 6.6 shows an excerpt of the studied IdMPs. According to their supported features, we indicated for which baseline they are appropriate. The Table shows that non of the listed IdMPs are appropriate for baseline *high*. For example, in case of *IBM*, it is because it does not support *purpose*, *pairwise* and *verified_claims* that are required to meet privacy goal *purpose specification*, *data unlinkability*, and *data minimization*, respectively.
- opt 2. *indicating discovery Endpoint URL*: the controller can provide the IdMP's discovery endpoint URL. The tool sends an HTTP Get request to the endpoint and receives a JSON response. The processor utilizes a *JSON parser* to extract truth values of the *af*, by mapping the $\langle \text{key}, \text{value} \rangle$ into $\langle af, T/F \rangle$. For example, the corresponding key to *cf Subject Type* is *subject_type_supported*. Table 6.7 represents the relation between $\mathcal{AF}_{idmp}$ and discovery endpoint JSON Keys.
- opt 3. *replying a questionnaire*: the controller can reply to a Yes/No questionnaire, called *IdMP_Doc Questionnaire*. To generate the questionnaire, we use the OAuth/OIDC reference model (see Section 6.2.1) that is stored in a database called *OAuth/OIDC ReferenceModel_DB*. For example, it asks "Does the IdMP

Table 6.6: An excerpt list of known IdMPs and their supported features.

Atomic Feature				
Code	✓	✓	✓	✓
Implicit	✓	✓	✗	✓
Client credential	✓	✗	✗	✗
Password	✓	✗	✗	✗
Hybrid	✓	✗	✗	✗
mTLS	✓	✗	✗	✗
Client_secret_basic	✓	✓	✓	✓
Client_secret_post	✓	✓	✓	✓
Client_secret_jwt	✗	✗	✗	✗
Private_key_jwt	✓	✗	✗	✗
Plain	✓ _{opt}	✓ _{opt}	✗	✗
S256	✓ _{opt}	✓ _{opt}	✗	✗
request	✓	✗	✗	✗
request_uri	✓	✗	✗	✗
query	✓	✓	✓	✓
Claim	✓	✗	✗	✗
Scope	✓	✓	✓	✓
Purpose	✗	✗	✗	✗
Verified Claims	✗	✗	✗	✗
Acr_values	✓	✗	✗	✗
vot	✗	✗	✗	✗
Public	✓	✓	NA	✓
Pairwise	✗	✗	NA	✗
Baseline	<i>low</i>	<i>low</i>	<i>low</i>	<i>low</i>
LEGEND: ✓ _{opt} : Supported, but not enforced, NA: Not applicable				

supports Implicit flow?”, “Does the IdMP support mTLS client authentication method?”. Please find the list of questions in Appendix D.4.

Note that the questionnaire gets updated according to the scenario, namely SSO or AD and the Flow, as follows: (i) in case of AD scenario, our tool filters out related questions to Subject Type, and Claims, verified claims, and purpose; and (ii) in case of Implicit flow, our tool filters out Code challenge method, Client Authentication and only keeps *af* query for the *cf* Response mode.

To provide a list of popular IdMPs, we studied the IdMPs listed in the OpenID Foundation website [Ope]. We considered the provided list for *Certified FAPI OIDC* for *high* and *moderate* baseline, and *certified OIDC Core* for baseline *low*. From which we have selected 19 IdMPs, according to their Alexa ranks and whether they have a free developer console to assess their features. To identify the truth values of their *afs*, we studied the available documentation and/or the developer console to assess their features. Table 6.6 provides an excerpt of the IdMPs we have studied; the full

Table 6.7: The Relation between IdMP features and Discovery Endpoint JSON Keys.

Feature	Discovery Response JSON Key
Response Type	response_type_supported
Client Authentication	Token_endpoint_auth_methods_supported
Code challenge	code_challenge_methods_supported
Request	request_uri_parameter_supported
	request_parameter_supported
Subject Type	subject_types_supported
Identity proofing	vot_values_supported
	acr_values_supported
claims	claims_parameter_supported
scope	Scops_supported
purpose	verified_claims_parameter_supported
verified_claims	

table is available in the Appendix D.3. Not surprisingly, we discovered that not all selected IdMPs provide appropriate level of security and privacy for all baseline, in particular for the *moderate* and *high* baseline. For instance, *Yahoo* does not support the following *afs*: Plain, S256, claims, purpose, acr, verified_claims and vot, while the *IBM solution* is appropriate for the *high* baseline. The database of known IdMPs gets updated whenever a new IdMP is introduced either via the discovery endpoint or the questionnaire. As a reliability check, the IdMPs listed in the database are tagged by their source, that is, *well-known*, *endpoint* and *questionnaire*. The level of reliability of the latter is lower.

The truth value of some $\mathcal{AF}_{\text{idmp}}$ cannot be identified neither through their documentation/free developer console nor the discovery endpoints. They can only be identified by the controller who is their client, such as nonce and state. To identify the truth values of such $\mathcal{AF}_{\text{idmp}}$, whenever the IdMP is identified from the list of well-know IdMPs or by the discovery endpoints (the first two options), we ask the controller to reply to a dynamically generated Yes/No questionnaire, called *IdMP_ToAsk_Questionnaire*. Moreover, the questionnaire asks about the *optional af*, that is, the features which are not activated by default by the IdMP. Thus, if the controller wants to implement them, s/he need to enable them from the IdMP console. For example, *IBM* has the *cf* Code challenge method (comprises of plain and S265) optional. The *IdMP_Doc Questionnaire* (the third option) already contains the questions that the *IdMP_ToAsk_Questionnaire* contains. To generate the questionnaire, the processor gets the OAuth/OIDC reference model (see Section 6.2.1), and filters out the already identified information. Please find the questionnaire in D.5.

Once The IdMP processor specified the *support_idmp* Boolean mapping for the em-

ployed *idmp*, it outputs a document, called *IdMP Specification*.

II. Client Processor The Client Processor aims to assess which $af \in \mathcal{AF}_{\text{common}} \cup \mathcal{AF}_{cl}$ have been implemented by the client *cl* in the OAuth/OIDC solution. More formally, it boils down to specify the $implement_{cl}$ Boolean mapping.

To support the controller in this process, our tool provides a Yes/No questionnaire, called *Client Implementation*. By leveraging the $support_{idmp}$ (obtained from the IdMP Processor), the processor automatically takes into account the choices that are constrained (as defined in Section 6.2.3) by the employed *idmp* and selects the relevant questions for the client. As such, we have first analyzed the employed IdMP for its *afs*, to not question the controller for the $\mathcal{AF}_{\text{common}}$ that the IdMP in question does not support, refer to as *False_AF_IdMP*. To customize the questionnaire accordingly, the processor takes *False_AF_IdMP* and drops them out of the questionnaire. Thus, the questionnaire asks controller about implementation of $\mathcal{AF}_{cl}$ and supported $\mathcal{AF}_{\text{common}}$.

The questionnaire dynamically updates, as follows:

- when the answer to one *af* of a *cf* is “Yes”, the questionnaire cancels out the questions on other *afs* of the *cf*, as the controller cannot implement more than one *af* of a *cf* for a given OAuth/OIDC solution;
- the $\mathcal{AF}_{cl}$ related questions gets updated by dropping:
 - Id_token_validation in case of AD scenario; and
 - distinct_redirect_URI in case of single IdMP.

Once the questionnaire is filled out, the processor outputs a document called *Client Specification*.

Application of the step on the scenario. The controller had selected *IBM* from the list of know *idmp*. As such, the *IdMP Processor* retrieves its truth values from the database (See Table 6.6). For the missing information, the controller replies the *IdMP_ToAsk_Questionnaire*. Following are the answers to the questionnaire. Note that, the controller did not activated the optional *cfcode* challenge method, which is *optional* for *IBM*.

Listing 6.1: The Answers to the IdMP_ToAsk_Questionnaire for IBM.

"fullRedirectURI.Support" : "F"	1
"patternRedirectURI.Support" : "T"	2

"nonce.Support" : "F"	3
"state.Support" : "T"	4
"formPost.Support" : "T"	5
"query.Support" : "T"	6
"fragment.Support" : "T"	7
"prompt_login.Support": "T"	8
"prompt_select_Account.Support": "T"	9
"prompt_consent.Support": "T"	10
"code_challenge_Method_plain.Support": "F"	11
"code_challenge_Method_S256.Support": "F"	12

While for *Barclays* the controller responded to the *IdMP_Doc Questionnaire*. Listing 6.2 represents the specification of the *Barclays* identified by the controller.

Listing 6.2: The Answers to IdMP_Doc Questionnaire for Barclays.

"token.Support" : "F"	1
"clientCredential.Support": "F"	2
"code.Support": "T"	3
"password.Support" : "F"	4
"hybrid.Support": "F"	5
"mTLS.Support" : "F"	6
"clientSecretJWT.Support" : "F"	7
"privateKeyJWT.Support" : "T"	8
"clientSecretBasic.Support" : "T"	9
"clientSecrtePost.Support" : "T"	10
"S256.Support" : "F"	11
"plain.Support" : "F"	12
"scope.Support" : "T"	13
"requestURI.Support": "T"	14
"request.Support" : "T"	15
"request_query.Support" : "T"	16
"fullRedirectURI.Support" : "T"	17
"Nonce.Support" : "T"	18
"State.Support" : "T"	19
"formPost.Support" : "T"	20
"query.Support" : "T"	21
"fragment.Support" : "T"	22
"prompt_login.Support": "T"	23
"prompt_select_Account.Support": "T"	24
"prompt_consent.Support": "T"	25

"vot.Support" : "F"	26
"acr.Support" : "T"	27

Then, the controller needs to indicated the implementation of both *IBM* and *Barclays* within his application. The *Client Processor* outputs Listing 6.3 for the *Barclays*, and Listing 6.4 for the *IBM*.

Listing 6.3: The Barcalys Implementation.

"Code.Implement": "T"	1
"clientSecretBasic.Implement": "T"	2
"request.Implement": "T"	3
"Nonce.Support": "T"	4
"State.Implement": "T"	5
"formPost.Implement": "T"	6
"scope.Implement": "T"	7
"fullRedirectURI.Implement" : "T"	8
"prompt_login.Implement": "T"	9
"acr.Implement": "T"	10
"Referrer.Implement": "T"	11
"Distinct_redirect_URI.Implement": "F"	12
"Open_redirect.Implement": "T"	13
"state_validation.Implement": "T"	14
"bind_IdMP_metadat.Implement: "T"	15
"store_IdMP_metadat.Implement: "T"	16
"iss_validation.Implement: "T"	17

Listing 6.4: The IBM Implementation.

"request. Implement: "T"	1
"state. Implement: "T"	2
"code. Implement: "T"	3
"client_Secret_basic. Implement: "T"	4
"claims. Implement: "T"	5
"acr. Implement: "T"	6
"prompt_consent. Implement: "T"	7
"public. Implement: "T"	8
"Id_Token_validation. Implement: "T"	9
"Form_Post. Implement: "T"	10
"Referrer. Implement:"F"	11
"Distinct_redirect_URI.Implement": "F"	12

"Open_redirect. Implement: "T"	13
"state_validation. Implement: "T"	14
"iss_validation.Implement: "T"	15
"bind_IdMP_metadat.Implement: "T"	16
"store_IdMP_metadat.Implement: "T"	17

III. Modeling and Evaluating Risk Using RiskML In the context of the OAuth/OIDC, a Risk model should contain risks posed by not-supported $\mathcal{CF}^*$ by IdMP and not-implemented $\mathcal{CF}^*$ by the client. These information are captured in *IdMP Specification* and *Client Specification* documents which represent the status of the employed IdMP solution. The RiskML captures them with the *expose* relation. However, to perform what-if analysis, they need to appear also with *protect* relation. To do so, we have generated a model which holds all *afs* regardless, called *OAuth/OIDC XML static File*. We customize it to model the solution in question, and call it *OAuth/OIDC Customized XML*. To have these two models, we introduce two components: *Static XML Generator* and *Customized XML Generator*, respectively.

We first elaborate on how RiskML language maps into the OAuth/OIDC. Then, we detail the process of generating the model.

RiskML Model. The RiskML model composed of a set of: *situations* that capture *afs*; *indicators* that indicates whether the *af* is implemented/supported—be set to 1 indicates that the *af* is implemented/supported, and 0 indicates otherwise; *events* that capture threats; and *goals* that captures goals. They are connected to one another with the following relations: *Indicate* (*i, s*), *Expose* (*s,e,w*), *Protect* (*s,e,w*), and *Impact*(*e,g,w*). The *Weight* on relation *expose* defines *likelihood*, and on *protect* defines the *protection* level. As mentioned, to evaluate protection and likelihood we sum the values, as *afs* contribute differently to the solution. For each, threat, we consider the maximum protection/likelihood it could have if all/no related *afs* are implemented.

Static XML Generator. The generator takes the *OAuth/OIDC ReferenceModel_DB* (see Section 6.2.1) to generate the *OAuth/OIDC XML static File*, that contains all $\mathcal{CF}^*$ s. It first generate a model considering all $\mathcal{CF}^*$ s are supported/implemented—that generates *protect* relation. In case of *cfs*, it considers all the *afs*. The *cf* inherits the protection value from the implemented *af*. Figure 6.3.a illustrates a part of generated *Static XML* model relates to *cf Code Challenge method* where its two *afs*, namely plain and S256 are modeled.

Then it updates the model, considering none of the $\mathcal{CF}^*$ s are supported/implemented—that generates *expose* relation. In case of *cf*, the model only contains the *cfs* without their *afs*. As, related threat(s) to *afs* raises if they are not supported/implemented,

while related threat(s) to a *cf* raises if none of its *afs* are supported/implemented; other words, when the *cf* is not supported/implemented. See again Figure 6.3.a where the Code challenge method appeared with *expose* relation, without its *afs*.

For controllers to capture who is the responsible of the posed threats, situations are labeled IdMP and C for IdMP_specific and client_specific, respectively. The weight of *protect* and *expose* relations are set according to the values set in the *OAuth/OIDC reference model*. While the weight of relation *impact* is taken from the variable *impactValue*. All the indicators of this model are set to 0. The left side of Figure 6.3.a captures the IdMP side—annotated with *_IdMP*, while the right-side is the client side, annotated with *_C*. The generated file inputs into *Customized XML Generator* to be customized for the solution in question.

The Generator regenerates the *OAuth/OIDC XML static File* whenever the *OAuth/OIDC reference model* gets updated.

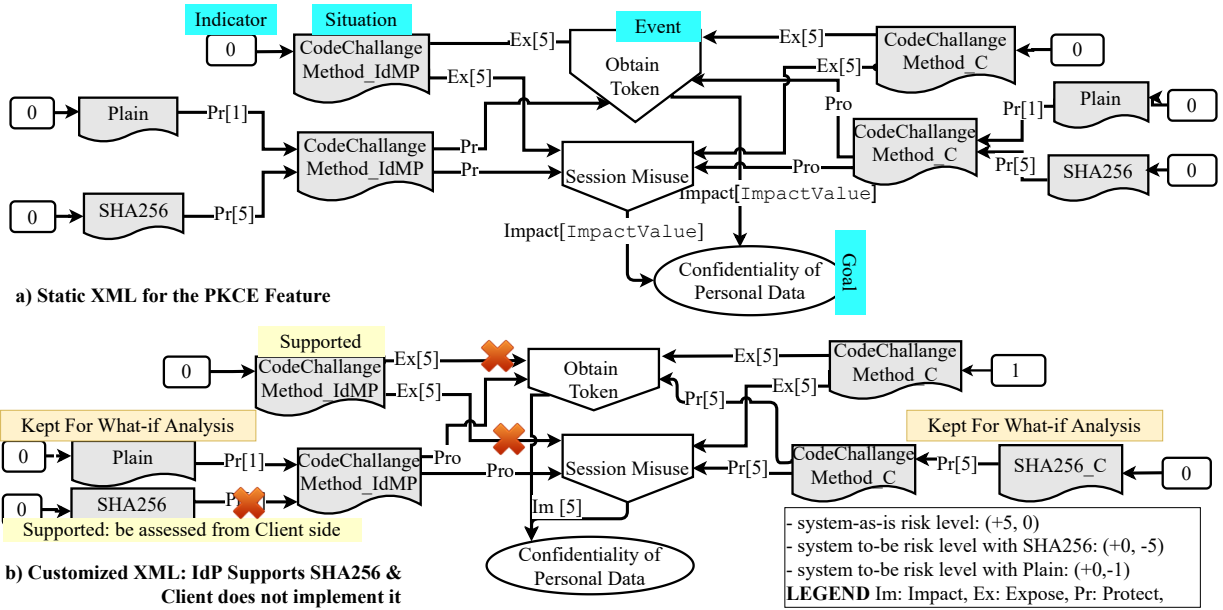


Figure 6.3: Static XML Model, Related to Feature Code Challenge Method

Customized XML Generator. The generator aims to generate an XML file that represents the solution as-is by customizing *Static XML File* based on the specification of the solution. Therefore, it takes as input *IdMP specifications* and *Client Specification* documents, according to which it sets the value of indicators. We call the situation with expose relation *expose-situation* and the ones with protect relation *protect-situations*. To model an implemented *cf*, it sets to 1 the indicators of the protect-situation representing its implemented *af*, while keeping the indicators of its other *af* to 0. And in the case of *af*, it sets to 1 the indicators of related protect-

situation. To model a not-supported/not-implemented $\mathcal{CF}^*$, the generator sets the indicator of related *expose-situation* to 1.

According to *IdMP specifications* the generator set only not-supported $\mathcal{CF}^*$ s to model the risk posed by IdMP, and leave the supported ones to be set according to *Client Specification*. Because a $\mathcal{CF}^*$ can be only useful if the client implements it. Note that this only holds for the AF_{common} . Figure 6.3.b illustrates the model for the scenario where the IdMP supports only SHA256 from the *cf* Code Challenge method. Thus from the IdMP-side, the generator drops the expose-situation representing *cf* Code Challenge method, and the supported-situation representing SHA256—it shall be assessed from the client side—while keeping the Plain for what-if analysis.

According to *Client Specification*, the generator sets: (i) indicator of implemented *afs*; and (ii) not implemented $\mathcal{CF}^*$ s. In the example modeled in Figure 6.3.b, the controller has not implement the only *af* supported for the *cf* Code Challenge, that is SHA256. Thus, the generator set the expose-situation representing the *cf* to 1, and kept the protect-situation representing SHA256 to perform what if analysis. Once these changes are made, the XML file represents the solution as-is. What remained unchanged—indicators set to 0—in the static XML file are the $\mathcal{CF}^*$ that are either: not-supported by the IdMP or not implemented by the controller. They remain for the controller to change their indicators to perform what-if analysis.

Performing What-if Analysis. The what-if analysis functionality allows controllers to make informed decisions about treatments to take, that are: choosing an IdMP which supports not-supported $\mathcal{CF}^*$ s by the employed one, and/or implementing the overlooked *afs*. The controller can perform the following what-if analysis:

1. what if the IdMP would support the *cf* that it does not?
2. what if the IdMP would support the *af* that it does not?
3. what if the controller had implemented the *af* s/he does not?
4. In case that the IdMP supports two *afs* for a *cf*, what if the controller had implemented one instead of the other?

To perform what-if analysis, the controller only needs to play with the value of indicators that are a slide-bar button. Setting the indicator of a support-situation related to a *af* of a *cf*, sets the others automatically to 0 (as one *af* can be impemeneted for a dolution); and setting the value of support-situation related to a $\mathcal{CF}^*$ to 1, sets its related expose-situation to 0.

Figure 6.3.b shows that in system as-is the risk level for goal *confidentiality of personal data* equals to (+5, −0). The controller could set the protect-situation SHA256

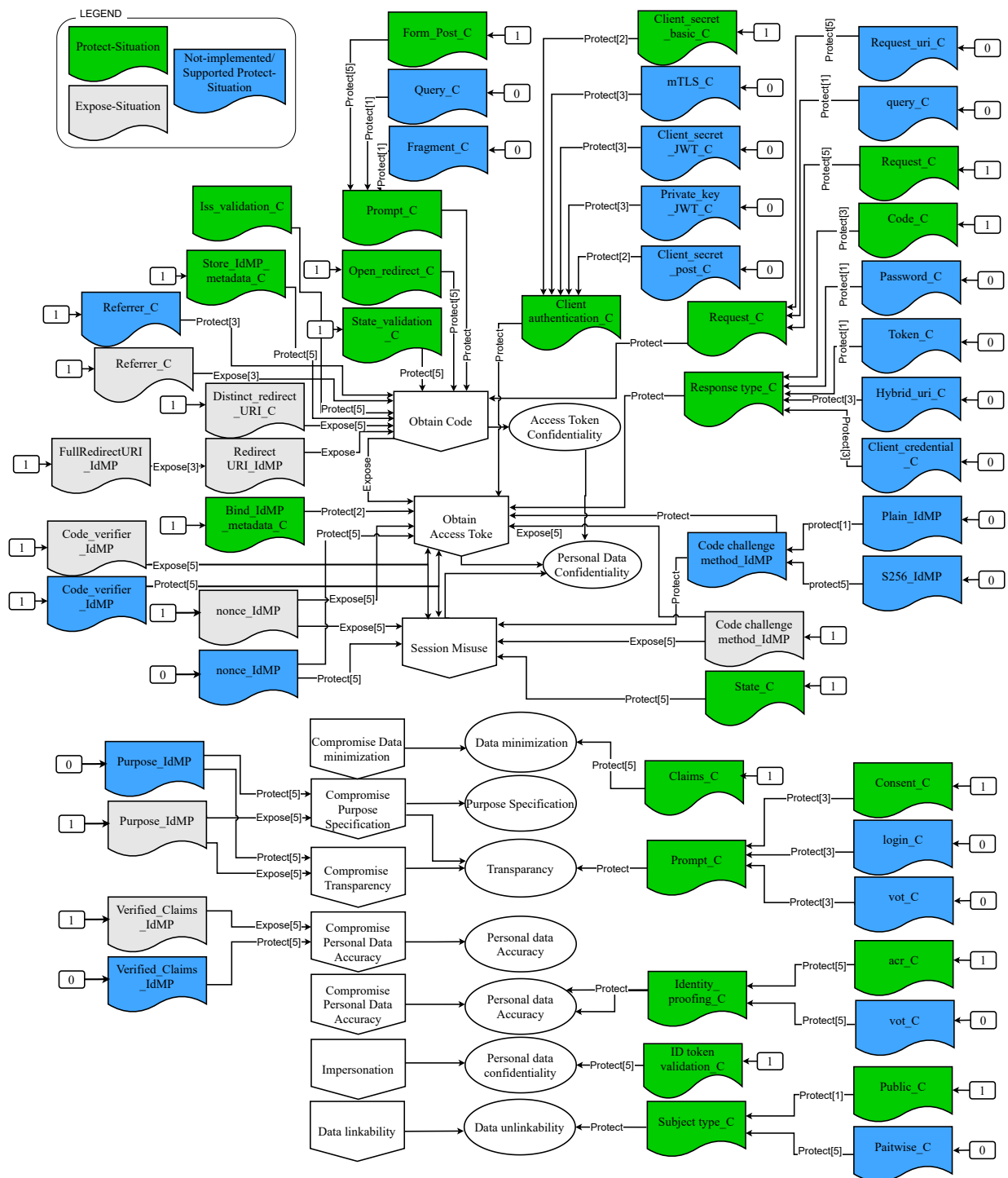


Figure 6.4: IBM Risk Model.

to 1, to see what is s/he has implemented it. That automatically set expose-situation *Code Challenge method_C* to 0, as implementing one *af* from a *cf* means there is no exposure coming from that *cf*. As SHA256 provide 5 level of protection, the risk level would be $(+0, -5)$. The controller could check what the risk level would be if the IdMP would have supported Plain and s/he had implemented it. That would set the expose-situation *Code Challenge_C* and protect-situation SHA256 from IdMP side to 0, as only one *af* could be implemented per request. As the Plain provides 1 level of protection, the risk level would be $(+0, -1)$.

Application of the step on the scenario. According to the *IdMP Specification* and *Client Specification*, the RiskML generates the model related to the implementation of the IBM. Figure 6.4 represents the Model. The evaluated impact of the scenario is 5 (See Section 6.3.1). To keep the model clean, we have dropped the impact values from *impact* relations (the relation between *event* and *goal*).

Following we provide two examples of the calculated risk level: the risk level of goal *Access token confidentiality* is $(+1., -3.9)$. As it is impacted by event *obtain code*, with likelihood level +1 because the following expose-situations hold:

- *Distinct_redirect_URI_C* (with likelihood level 5),
- *Referrer_C* (with likelihood level 3);

and protection level -3.9 , because the following protect-situations hold:

- *pattern_redirect_URI_IdMP* of *cf redirect_URI_IdMP* (with protection level 1),
- *Open_redirect_C* (with protection level 5),
- *Store_IdMP_metadata_C* (with protection level 5),
- *State_validation_C* (with protection level 5),
- *Iss_validation_C* (with protection level 5),
- *af Request* of *cf Request_C* (with protection level 5);
- *af Form_Post* of *cf Prompt_C* (with protection level 5).

the risk level of goal *Transparency* is $(+3.1, -1.9)$. It is impacted by event *Compromise transparency*, for which the expose-situation *Purpose_IdMP* (with likelihood level 5), and protect-situation *Consent* from *cf Prompt_C* (with protection level 3) holds.

Following we give two examples of what-if analysis on the IBM model:

1. What if the IBM would support *nonce* that it does not? *Nonce_IdMP* protect the system from the exposure of event *session misuse*, that its likelihood level in system as-is is +3.75 (exposed by situation *nonce_IdMP* (with likelihood level +5), *Code challenge method_IdMP* (with likelihood level +5), and *Code_verifier_IdMP* (with likelihood level +5)); and protection level -1.25 (protected by *State_C* (with protection level -5)). If the *nonce_IdMP* was supported and implemented, the likelihood level of mentioned event will decrease to +2.5, and the protection level will increase to -2.5.

Nonce_IdMP also protect the system from the exposure of event *Obtain access token*. The likelihood level of the event in system as-is is +1.9 (exposed by situation *Nonce_IdMP* (with likelihood level +5), *Code challenge method_C* (with likelihood level +5), *Code_verifier_IdMP* (with likelihood level +5), and event *Obtain Code* (with likelihood level +1)); and its protection level is -3 (protected by *Bind_IdMP_metadata_C* (with protection level 3), *af code of cf Request_C* (with protection level 3), *af Client_secret_basic_C* of *cf Client authentication_C* (with protection level 2), and goal *Access Token Confidentiality* (with protection level 3.9) If the *nonce_IdMP* was supported and implemented, the likelihood level of mentioned event will decrease to +1.4, and the protection level will increase to -3.4.

2. what if the controller had implemented the *Code challenge method_C* s/he does not?

The *Code challenge method_C* is a *cf*, comprises of two *afs*: *Plain* and *S256*. and it protects the system from the exposure of *session misuse* and *Obtain access token*. Let us consider its impact on *session misuse* with likelihood level +3.75 and protection level -1.25.

If the controller would have implemented *plain*, the level had been 1.5 and 3.5, respectively. While if he would have implemented *S256*, the level had been 2.5 and 2.5, respectively.

6.3.2.2 Addressing $P_{compliance}$

To assist controller, our tool raises warning when: (i) employed IdMP does not support BCP requirements of the baseline, and (ii) controller does not implement the BCPs supported by the IdMP ($\mathcal{AF}_{common}$), or the $\mathcal{AF}_{cl}$ related BCP. To do so, we introduced three components, called *IdMP BCP Checker*, *Controller BCP Checker* and *BCP Extractor*. The latter prepares the inputs for the checkers, that is, to extract the related BCPs of a given baseline for IdMP and client from *BCP_DB*. The database called *BCP_DB* stores all the BCPs discussed in this section. As such, it takes as input a *BCP_DB* (see Section 6.2.2) and the baseline from variable *ProcessingBaseline*.

IdMP BCP Checker. The Checker gets as input common and IdMP related *BCPs* of the baseline, and the *IdMP Specification* document. The checkers check the specification of employed IdMP against the output of the BCPs for its compliance.

Client BCP Checker . The controller should not get a warning for the common features that the IdMP does not support. To cancel them out from the client BCPs, the checker has a component called *BCP filter*. It takes as input the *False_AF_IdMP* and drops them from related BCP. The *Client BCP Checker* checks the *Client Specification* against the output of the filter to verify whether the controller has implemented the BCPs of the baseline to raise a warning for overlooked ones.

Application of the step on the scenario. The baseline of the scenario is *High*. As such the employed IdMPs need to comply with the FAPI BCPs.

The *IdMP BCP Checker* raise warning for following overlooked $\mathcal{CF}^*$ s: *Nonce*, *pairwise*, *purpose*, *verified_claim*, and *Full_redirect_URI* by *IBM*; and *Code Challenge* method by *Barclays*.

The *client BCP Checker* raise warning for following overlooked $\mathcal{CF}^*$ s by *IBM*: *distinct_redirect_URI* and *Referrer*; and *distinct_redirect_URI* for *Barclays*.

6.4 Related Work

Birrell and Schneider [BS13] discussed different design choices to enforce the following privacy goals: *Undetectability*, *Unlinkability*, and *Confidentiality*. They discuss that enforcing the goals depends both on system design and the interaction of service providers with an identity management system.

Werner and WeWestphall [WW16] proposed an identity management model for cloud environments that aims to reduce the risks of breaching privacy by enforcing *transparency*, *controllability* and *data minimization*. Their model allows users to define a privacy policy to regulate the use and dissemination of data. IdMP sent the defined policy to service providers; the provider ensures that policies representing user preferences will be accomplished.

Weingartner and Westphall [WW17] proposed an approach to enforce privacy goals *confidentiality*, *interveinability*, *transparency* and *accuracy*. For that, it requires users to encrypt their personal data before sending to IdMP, and allows users to select which attributes to disclose as they need to open the encrypted data to disclose to controllers. It also provides a Validation Process to validate user's attributes before IdMP stores them. This process happens once for each personal data, such

as email addresses, social security and credit card numbers and any other sensitive data. They state that any Civil registration agencies, banks, and other governmental and non-governmental agencies which issue user data can act as a validation service.

EL PASSO [ZKS⁺20] offers an easy-to-deploy (for both IdMP and controller) asynchronous and unlinkable authentication. It aims to fulfill the following privacy goals: *data minimization*, *intervenability*, and *user accountability*. To fulfill them, EL PASSO avoids synchronous communication between controllers and IdPs. EL PASSO has the following contributions: disallows controller and IdMP to track the user, allows user to disclose his personal data selectively, and holds misbehaving users accountable in cooperation with law enforcement authorities.

Navas et al. [NB19] proposed a threat modeling for the OIDC core specification by highlighting both security and privacy goals, such as: *confidentiality*, *integrity*, and *interveinability*. They require to encrypt personal data (by a procedure on users' side) before sharing with IdMP, which needs to be validated by a trusted third party. To mitigate user/controller impersonation they modify format of token by adding `sub_IP`, `aud_IP`, `public_key`, and bind it to the user's certificate, respectively.

Wanpeng et al. [LM20] performed a systematic analysis of the user access privacy in the OAuth and consequently, OIDC standards. The analysis revealed that to make the protocol thoroughly privacy-friendly, it demands fundamental changes to how they operate.

Authors in [HSB20] propose an extension to OIDC to prevent colluding clients by proposing a new design of pairwise parameter, honest but curious IdMPs attacks, by using a cryptographic hash function to mask controller identifier. They make user agent capable of masking controllers' identifiers and obtaining consent instead of IdMP. They collaborate with the OpenID Foundation to provide a reference implementation.

Wanpeng et al. [LM20] performed a systematic analysis of the user access privacy in the OAuth and OIDC standards. They believe that making the protocols privacy-friendly requires fundamental operational changes, as privacy has not been considered in the protocols' design. Similar to [HSB20], they investigated the ways IdMPs can track during login and user information retrieval; and suggest a client-based mitigation strategy that acts as an intermediary between the controller and IdPs to transmit the authorization requests/responses. They highlight that the main cause of user tracking by IdMPs is due to the controller pre-registration phase, where they reveals security-critical information, such as `client_id` and `redirect_uris` that enables IdPs to identify controller that the user tries to connect.

Authors in [PM12] surveyed the current approaches for addressing privacy in iden-

tity management systems. They list privacy requirements and discuss how the currently deployed systems address them. They state an identity management system need to address the following to be privacy-friendly: (i) trust model; (ii) multiple unlikable identities; (iii) selective disclosure; (iv) consent; and (v) privacy-respecting sharing of personal information. Their analysis revealed that: *SAML 2.0* revealed that it does not support selective disclosure by default, as it on IdMP to provide a user interface to define selective disclosure policy; *CardSpace* system provides a mechanism to reduce the trust requirement on the IdMPs, and so prevents IdMPs to monitor users activity; *eID* (that is the most recent identity management system that is the electronic equivalent of citizens national identity cards), except the German eID system, fails to provide a complete privacy-preserving solution due to revealing more information than is strictly necessary; they claim *OpenID* does not support any degree of anonymity or pseudonymity due to the issuance of a global identifier for user authentication and hence is much less privacy-friendly. Their analysis and findings introduce PrimeLife and TAS3 projects, which are the latest ongoing European research projects aiming to improve privacy in identity management systems.

6.4.0.1 Discussion

To provide security and privacy most of the available research works in the wild: (i) demands fundamental changes to the way that protocol operates; and (ii) proposes browser-based solutions or adding cryptographic functions.

What these works have in common is that they either: (i) demands fundamental changes to the way that protocol operates; and/or (ii) proposes browser-based solutions or adding cryptographic functions. They require major changes in IdMPs and the client's current implementation, time to adapt, and computational overhead. Whereas our methodology utilizes existing OAuth/OIDC features and It cannot prevent honest but curious IdMP attack, in any case.

6.5 Conclusion

Conducting a DPIA-compliant risk analysis for OAuth/OIDC solutions is complex. We break the complexity into two problems: security and privacy risk analysis (P_{risk}) and compliance with the IdMP security and privacy BCPs ($P_{compliance}$). We adapted the second step of our methodology to address these problems. To do that, we have built a reference model from the OAuth/OIDC security and privacy-related components. The model assists the automatic assessment of IdMPs deployment and their integration within the client—considering the client's security and privacy in ques-

tion. The assessment output will be fed into the RiskML tool to model the system and automatically perform what-if analysis automatically. The analysis enables controllers to make an informed decision on their choice of IdMP and implementation to eliminate identified risks or minimize their impact.

Chapter 7

Conclusion

Any organization or service provider that processes personal data shall comply with the GDPR. In article 5, the GDPR introduces data processing principles, and mandates controllers to follow them. Article 12 to 22 introduce data subjects rights which controller shall respect. Article 83.5.a and b states that infringements of the principles and the rights are subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. Recital 76, article 24 and 32 mandates controllers to evaluate risks to rights and freedoms of data subjects concerning the processing of their personal data, and to implement appropriate technical and organizational measures to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services. When data processing is likely to result in high risks to data subjects' rights and freedoms, article 35 mandates controllers to conduct a Data Protection Impact Assessment (DPIA). It is not clear when and how a DPIA shall be conducted. [oAIC14, VvdB17] discuss that it is the case for most of data processing. [Arta] state that where it is not clear whether a DPIA is required, a DPIA is carried out nonetheless; as a DPIA is a useful tool to help controllers comply with data protection law. Moreover, along with article 35, other articles of the GDPR, mentioned above, require to evaluate risks to data subjects' rights and freedoms and introduce measures to treat them.

A GDPR-compliant risk assessment shall assess both security risks, that is risks to compromising the CIA triad, and privacy risks, that is risks to rights and freedoms of data subjects (e.g., risk to reputation, social life or losing control over ones' data). However, assessing the latter is not trivial and it is subjective. The EDPB states that for managing such risks controllers need to take data subjects' perspective [Arta]. Different scholars discussed that people are not aware of privacy risks (see e.g., [SV14, GRV19]), while others believe that people are aware of privacy

risks(see e.g., [Sol20]); they take context-aware decisions about accepting certain risk levels. Identifying privacy risks became mandatory with the GDPR, as such, information security and data protection experts, too, may not be aware of them. Given that, we have conducted two surveys to examine how lay people perceive privacy risks and whether security and privacy experts can differentiate privacy risks from security risks. We found out that awareness helps participants with better estimate of privacy impact, if proper communication method are used. Beside, experts confuse security risks with privacy risks. Chapter 3 discussed the surveys and their results.

To comply with the requirements of the DPIA, Controllers need to: (i) evaluate the risks to rights and freedoms of data subjects—which is uneasy to identify—(ii) assess the impact of the envisaged processing operations on the protection of personal data—when its process is unclear—and (iii) implement appropriate technical and organizational measures to ensure an appropriate level of security—when realizing the appropriate security level is not trivial. Meeting such requirements is a daunting task on the shoulder of controllers (Chapter 2 has discussed and formulated these problems). To assist them, we have proposed an assisted methodology to guide controllers to conduct a DPIA. It examines whether the data processing in question respects data processing principles and data subjects’ rights. It assists controllers in identifying both privacy and security risks and guides them to introduce countermeasures. By enabling the controller to perform what-if analysis, it allows them to decide how to preserve the security and privacy of the system. Chapter 5 has detailed the methodology and the assistance it provides.

People’s engagement in online services is growing; along with that the amount of shared personal data and the risks such as loss or theft of personal data, data protection violations, etc. Open banking—which is pushed into the mainstream by regulatory changes—is not an exception. One of the key points to make these services trustworthy is to deploy an appropriate identity management solution. Among other identity management solutions, OAuth 2.0 (OAuth) and OpenID Connect (OIDC) are two widely used ones (as stated also in [Sim, LM20])—but error-prone. Personal data are involved in the authentication and authorization process; moreover, they could be a gateway to access a special category of data. For example, recently, the internet bank account takeover of +1M users without user interaction due to an implementation flaw within their OAuth solution [Kre]. As such, it is crucial to conduct a DPIA-compliance risk analysis for OAuth/OIDC-based solutions. However, it is a complex task because it requires controllers to: (1) assess risks for both IdMP’s deployment and clients side, which requires them to (2) face a maze of documents and guidelines to perform such risk assessment; (3) be aware of security and privacy requirements of the client in question, and (4) of the DPIA. To assist controllers in performing a DPIA-compliance risk analysis, we have adopted our methodology to

consider all the above-mentioned requirements. Chapter 6 explained the adoption of our methodology.

In summary, our proposed methodology aims to assist controllers to comply with the requirements of the DPIA, from specifying the data type necessary for the data processing to identify security and privacy risks. We have proposed security and privacy reference models based on which controllers could assess whether the system meets the appropriate level of security for their system and privacy requirements. By conducting a what-if analysis, our methodology allows the controller to identify a configuration for their system that minimizes the risk level. We have then adopted our methodology to conduct the DPIA for the identity management solutions, in particular for OAuth/OIDC protocols. We have proposed a security and privacy reference model for OAuth/OIDC protocols, as well.

7.1 Future Work

The DPIA is a “living” document [WFR13], it should be continuously reviewed and regularly re-assessed [Arta]; which is the aim of the third step of our methodology, namely *Run-time Analysis* (see Figure 5.1). To do that, we plan to investigate combining data analytic techniques with selected monitoring tools—such as those for Inventory Management (IM) and Security Information and Event Management (SIEM).

To conduct a more comprehensive risk analysis for OAuth/OIDC-based services, we plan to consider the interrelations between atomic features that impact their contributions to securing the solution. For example, consider that the client uses `code_challenge_method` for some flows (e.g., pure-OAuth flows) and `Nonce` for other flows (e.g., those using OpenID Connect) at the same authorization server within its authorization request. If an attacker steals an authorization code that is bound to a `Nonce`, s/he could inject the obtained code into a pure-OAuth authorization flow that uses `code_challenge_method` to obtain an `access_token` by sending a not matching code challenge. As such, the usage of `code_challenge_method` does not help to protect the authorization flow from the threat *obtaining code*, as the client’s implementation contains a dynamic switch between the `code_challenge_method` and `Nonce`.

Web services security dimensions have been defined as: secure communication, resource protection, negotiation of contracts, trust management, and security properties [SWS07]. Secure communication is becoming more and more important and relevant in open banking contexts, where ensuring ongoing confidentiality, integrity

and resilience are crucial. We have assessed the level of security and privacy for the OAuth/OIDC-based authentication and authorization process (see Chapter 6) to ensure that it provides an appropriate level related to the service in question. We plan to further investigate secure communication by building a relevant Reference Model to ensure a minimum level of security and privacy for a given scenario and guiding controllers to integrate information security practices. The Reference Model will contain the TLS components (e.g., openssl, cipher suit, certificate validations). The model will be used to identify the implemented components for the service in question. Its aim is two-folded: (i) to check possible vulnerability of the components, and (ii) to model and evaluate risk level. For example, openssl is one of the components which is an open-source implementation of the SSL and TLS protocols. OpenSSL 1.0.1 before 1.0.1g suffers from the Heartbleed bug, which is a security bug in the OpenSSL cryptography library that allows remote attackers to obtain sensitive information from process memory (CVE-2014-0160). As such, we can have a comprehensive risk model and evaluation, considering both OAuth/OIDC and TLS integration. The input to our analysis can come from the existing tool (see e.g., [fet](#)) which runs an automatic analysis and provides suggestions to address them.

Bibliography

- [291] ISO/IEC 29100:2011. Information technology—security technique—privacy framework. <https://www.iso.org/obp/ui/#iso:std:iso-iec:29100:ed-1:v1:en>.
- [ACDC⁺15] Rehab Alnemr, Erdal Cayirci, Lorenzo Dalla Corte, Alexandr Garaga, Ronald Leenes, Rodney Mhungu, Siani Pearson, Chris Reed, Anderson Santana de Oliveira, and Dimitra Stefanatou. A data protection impact assessment methodology for cloud. In *Annual Privacy Forum*. Springer, 2015.
- [ACR99] Mark S Ackerman, Lorrie Faith Cranor, and Joseph Reagle. Privacy in e-commerce: examining user scenarios and privacy preferences. In *Proceedings of the 1st ACM EC*, 1999.
- [AEY10] Annie I Antón, Julia B Earp, and Jessica D Young. How internet users’ privacy concerns have evolved since 2002. *IEEE S & P*, 8, 2010.
- [Ahm20] Amirshayan Ahmadian. *Model-Based Privacy by Design*. PhD thesis, Universität Koblenz-Landau, 2020.
- [Alt75] Irwin Altman. The environment and social behavior: Privacy, personal space, territory, and crowding. 1975.
- [ANG17] Angeliki Aktypi, Jason RC Nurse, and Michael Goldsmith. Unwinding ariadne’s identity thread: Privacy risks with fitness trackers and online social networks. In *Proceedings of MPS*. 2017.
- [Arta] Article 29 Working Party. Guidelines on data protection impact assessment and determining whether processing is “likely to result in a high risk” for the purposes of regulation 2016/679. <https://ec.europa.eu/newsroom/article29/items/611236>. Accessed: 2021-05-16.

- [Artb] Article 29 Working Party. Opinion 07/2013 on the data protection impact assessment template for smart grid and smart metering systems ('DPIA template') prepared by expert group 2 of the commission's smart grid task force. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp209_en.pdf. Accessed: 2019-19-06.
- [Artc] Article 29 Working Party. Opinion 5/2010 on the industry proposal for a privacy and data protection impact assessment framework for RFID applications. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp175_en.pdf. Accessed: 2019-19-06.
- [AS17] M Alshammari and AC Simpson. Towards an effective PIA-based risk analysis: an approach for analysing potential privacy risks. Technical Report CS-RR-18-01, Department of Computer Science, University of Oxford, 2017.
- [ASRJ18] Amir Shayan Ahmadian, Daniel Strüber, Volker Riediger, and Jan Jürjens. Supporting privacy impact assessment by model-based privacy analysis. In *Proceedings of the 33rd Annual ACM Symposium on Applied Computing*, pages 1467–1474, 2018.
- [ATW16] Alessandro Acquisti, Curtis Taylor, and Liad Wagman. The economics of privacy. *JEL*, 54, 2016.
- [BB18] Jaspreet Bhatia and Travis D Breaux. Empirical measurement of perceived privacy risk. *ACM TOCHI*, 25, 2018.
- [BEL17] Fredrik Blix, Salah Addin Elshekeil, and Saran Laoyookhong. Data protection by design in systems development: From legal requirements to technical solutions. In *12th International Conference for Internet Technology and Secured Transactions*, pages 98–103. IEEE, 2017.
- [BFH⁺16] Felix Bieker, Michael Friedewald, Marit Hansen, Hannah Obersteller, and Martin Rost. A process for data protection impact assessment under the European general data protection regulation. In *Annual Privacy Forum*, pages 21–37. Springer, 2016.
- [BG⁺10] Gaurav Bansal, David Gefen, et al. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision support systems*, 49, 2010.

- [BGL⁺17] S Brooks, M Garcia, N Lefkovitz, S Lightman, and E Nadeau. Nistir 8062. an introduction to privacy engineering and risk management in federal systems. *Information Technology Laboratory, National Institute of Standards and Technology*, 2017.
- [BHS⁺16] Xavier Bellekens, Andrew Hamilton, Preetila Seeam, Kamila Nieradzinska, Quentin Franssen, and Amar Seeam. Pervasive eHealth services a security and privacy risk awareness survey. In *CyberSA*. IEEE, 2016.
- [BMA94] Paul N Bloom, George R Milne, and Robert Adler. Avoiding misuse of new information technologies: legal and societal considerations. *The Journal of Marketing*, pages 98–110, 1994.
- [BN18] Elizabeth E Bruch and MEJ Newman. Aspirational pursuit of mates in online dating markets. *Science Advances*, 4, 2018.
- [BO] Bob Byers and Harold Owen. Automation support for cve retrieval. <https://csrc.nist.gov/CSRC/media/Projects/National-Vulnerability-Database/documents/web%20service%20documentation/Automation%20Support%20for%20CVE%20Retrieval.pdf>. Accessed: 2021-04-08.
- [Boa] European Data Protection Board. Guidelines on data protection officers (‘DPOs’).
- [BPJR07] Tom Buchanan, Carina Paine, Adam N Joinson, and Ulf-Dietrich Reips. Development of measures of online privacy concern and protection for use on the Internet. *JASIST*, 58, 2007.
- [BS13] Eleanor Birrell and Fred B Schneider. Federated identity management systems: A privacy-based characterization. *IEEE security & privacy*, 11(5):36–48, 2013.
- [Cam09] L Jean Camp. Mental models of privacy and security. *IEEE Technology and society magazine*, 28, 2009.
- [CFKA18] Joshua Coles, Shamal Faily, and Duncan Ki-Aries. Tool-supporting data protection impact assessments with CAIRIS. In *5th International Workshop on Evolving Security & Privacy Requirements Engineering*, pages 21–27. IEEE, 2018.
- [CG14] Kovila PL Coopamootoo and Thomas Groß. Mental models for usable privacy: A position paper. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*. Springer, 2014.

- [CG⁺16] A Crespo Garcia et al. Pripare. *Privacy-and Security-by design Methodology Handbook*, 2016.
- [Cha17] Lik Sam Chan. Who uses dating apps? exploring the relationships among trust, sensation-seeking, smartphone use, and the intent to use dating apps based on the integrative model. *COHB*, 72, 2017.
- [CHH16] Michael Colesky, Jaap-Henk Hoepman, and Christiaan Hillen. A critical analysis of privacy design strategies. In *2016 IEEE Security and Privacy Workshops*, pages 33–40, 2016.
- [CK13] Colette Cuijpers and Bert-Jaap Koops. Smart metering and privacy in europe: lessons from the Dutch case. In *European data protection: coming of age*, pages 269–293. Springer, 2013.
- [Cla99] Roger Clarke. Privacy impact assessments. <http://www.xamax.com.au/DV/PIA.html/>, 1999. Accessed: 2019-22-10.
- [Cla09] Roger Clarke. Privacy impact assessment: Its origins and development. *Computer law & security review*, 25(2):123–135, 2009.
- [CM07] Sally Jo Cunningham and Masood Masoodian. Management and usage of large personal music and photo collections. In *IADIS-ICWI*, 2007.
- [CNI] CNIL (Commission Nationale de l’Informatique et des Libertés). The open source pia software helps to carry out data protection impact assesment. <https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment>. Accessed: 2020-02-25.
- [CNI12a] CNIL (Commission Nationale de l’Informatique et des Libertés). Methodology for privacy risk management: How to implement the data protection act. <https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf>, 2012.
- [CNI12b] CNIL (Commission Nationale de l’Informatique et des Libertés). Privacy impact assessment (PIA): Knowledge bases. <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf>, 2012.
- [CNI15] CNIL (Commission Nationale de l’Informatique et des Libertés). How to carry out a PIA. <https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf>, 2015.

- [CNI18] CNIL (Commission Nationale de l'Informatique et des Libertés). Privacy risk assessment (PIA). <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf>, 2018.
- [CNI01a] CNIL (Commission Nationale de l'Informatique et des Libertés). Methodology for privacy risk management. <https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf>, 2012, Accessed: 2020-09-01.
- [CNI01b] CNIL (Commission Nationale de l'Informatique et des Libertés). How to carry out a PIA. <https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf>, 2015, Accessed: 2020-09-01.
- [CNI01c] CNIL (Commission Nationale de l'Informatique et des Libertés). Privacy risk assessment (PIA). <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf>, 2018, Accessed: 2020-09-01.
- [Con17] Conference of the independent data protection authorities of the Federal and State Governments of Germany. The standard data protection model, v.1.0 EN1., 2017.
- [CRA00] Lorrie Faith Cranor, Joseph Reagle, and Mark S Ackerman. Beyond concern: Understanding net users' attitudes about online privacy. *The Internet upheaval: raising questions, seeking answers in communications policy*, 2000.
- [DDFH⁺15] George Danezis, Josep Domingo-Ferrer, Marit Hansen, Jaap-Henk Hoepman, Daniel Le Metayer, Rodica Tîrtea, and Stefan Schiffner. Privacy and data protection by design-from policy to engineering. *arXiv preprint arXiv:1501.03726*, 2015.
- [Dem19] Katerina Demetzou. Data protection impact assessment: A tool for accountability and the unclarified concept of 'high risk'in the general data protection regulation. *Computer Law & Security Review*, 35(6):105342, 2019.
- [DFJS07] S. De Capitani di Vimercati, S. Foresti, S. Jajodia, and P. Samarati. Access control policies and languages. *JCSE*, 3(2):94–102, 2007.
- [DFKA⁺20] Nicolás E Díaz Ferreyra, Tobias Kroll, Esma Aïmeur, Stefan Stieglitz, and Maritta Heisel. Preventative nudges: Introducing risk cues for supporting online self-disclosure decisions. *Information*, 11, 2020.

- [DH06] Tamara Dinev and Paul Hart. An extended privacy calculus model for e-commerce transactions. *ISR*, 17, 2006.
- [DJ16] Claas Digmayer and Eva-Maria Jakobs. Risk perception of complex technology innovations: Perspectives of experts and laymen. In *ProComm*. IEEE, 2016.
- [DLM16] Sourya Joyee De and Daniel Le Métayer. Priam: a privacy risk analysis methodology. In *Data Privacy Management and Security Assurance*, pages 221–229. Springer, 2016.
- [DLM17] Sourya Joyee De and Daniel Le Métayer. A refinement approach for the reuse of privacy risk analysis results. In *Annual Privacy Forum*, pages 52–83. Springer, 2017.
- [DM05] Roger Dingledine and Nick Mathewson. Anonymity loves company: usability and the network effect. designing security systems that people can use. *O’Reilly Media*, 2005.
- [DMGR15] Riccardo De Masellis, Chiara Ghidini, and Silvio Ranise. A declarative framework for specifying and enforcing purpose-aware policies. In *International Workshop on Security and Trust Management*, pages 55–71. Springer, 2015.
- [DR20a] Salimeh Dashti and Silvio Ranise. Tool-assisted risk analysis for data protection impact assessment. In *privacy and identity management*, pages 308–324. Springer, 2020.
- [DR20b] Salimeh Dashti and Silvio Ranise. Tool-assisted risk analysis for data protection impact assessment. *Privacy and Identity Management*, page 308, 2020.
- [DSCR21] Salimeh Dashti, Amir Sharif, Roberto Carbone, and Silvio Ranise. Automated risk assessment and trade-off analysis of OpenID connect and OAuth 2.0 deployments. In *Conference on data and applications security and privacy*, 2021.
- [DSDOK⁺21] Salimeh Dashti, Anderson Santana De Oliveria, Caelin Kaplan, Manuel Dalcastagnè, and Silvio Ranise. Can data subject perception of privacy risks be useful in a data protection impact assessment? In *18th International Conference on Security and Cryptography*, 2021.
- [DWS⁺11] Mina Deng, Kim Wuyts, Riccardo Scandariato, Bart Preneel, and Wouter Joosen. A privacy threat analysis framework: supporting the

- elicitation and fulfillment of privacy requirements. *Requirements Engineering*, 16(1):3–32, 2011.
- [eID14] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, 2014.
- [fet] Daniel fett. Finding and fixing tls misconfigurations with tls profiler. <https://danielfett.de/2020/05/22/open-source-tls-scanner/>. Accessed: 2021-05-12.
- [FGK13] Jesús Friginal, Jérémie Guiochet, and Marc-Olivier Killijian. Towards a privacy risk assessment methodology for location-based systems. In *International Conference on Mobile and Ubiquitous Systems: Computing, Networking, and Services*, pages 748–753. Springer, 2013.
- [FKM⁺15] Xavier Franch, Ron Kenett, Fabio Mancinelli, Angelo Susi, David Ameller, Maria Carmela Annosi, Ron Ben-Jacob, Yehuda Blumenfeld, OH Franco, Daniel Gross, et al. The riscoss platform for risk management in open source software adoption. In *IFIP International Conference on Open Source Systems*, pages 124–133. Springer, 2015.
- [FKS16] Daniel Fett, Ralf Küsters, and Guido Schmitz. A comprehensive formal security analysis of oauth 2.0. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 1204–1215, 2016.
- [FKS17] Daniel Fett, Ralf Küsters, and Guido Schmitz. The web sso standard openid connect: In-depth formal security analysis and security guidelines. In *2017 IEEE 30th Computer Security Foundations Symposium (CSF)*, pages 189–202. IEEE, 2017.
- [FSL⁺78] Baruch Fischhoff, Paul Slovic, Sarah Lichtenstein, Stephen Read, and Barbara Combs. How safe is safe enough? a psychometric study of attitudes towards technological risks and benefits. *Policy sciences*, 9, 1978.
- [GBO18] Christos Giakoumopoulos, Giovanni Buttarelli, and Michael O’Flaherty. Handbook on european data protection law. *Luxembourg: Publications Office of the European Union*, 2018.
- [GC12] Vaibhav Garg and Jean Camp. End user perception of online risk under uncertainty. In *45th HICSS*. IEEE, 2012.

- [GC13] Vaibhav Garg and Jean Camp. Heuristics and biases: implications for security design. *IEEE Technology and Society Magazine*, 32, 2013.
- [GCCLH12] Vaibhav Garg, L Jean Camp, Katherine Connelly, and Lesa Lorenzen-Huber. Risk communication design: Video vs. text. In *International Symposium on PET*. Springer, 2012.
- [GDP16] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data,, 2016.
- [GEL11] Jennifer L Gibbs, Nicole B Ellison, and Chih-Hui Lai. First comes love, then comes google: An investigation of uncertainty reduction strategies and self-disclosure in online dating. *Communication Research*, 38, 2011.
- [GRS17] Paolo Guarda, Silvio Ranise, and Hari Siswantoro. Security analysis and legal compliance checking for the design of privacy-friendly information systems. In *Proceedings of the 22nd ACM on Symposium on Access Control Models and Technologies*, pages 247–254, 2017.
- [GRV19] Nina Gerber, Benjamin Reinheimer, and Melanie Volkamer. Investigating people’s privacy risk perception. *Proceedings on PET*, 2019, 2019.
- [GTD11] Seda Gürses, Carmela Troncoso, and Claudia Diaz. Engineering privacy by design. *Computers, Privacy & Data Protection*, 14(3):25, 2011.
- [Han11] Marit Hansen. Top 10 mistakes in system design from a privacy perspective and privacy protection goals. In *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life*, pages 14–31. Springer, 2011.
- [Har12] Dick Hardt. The oauth 2.0 authorization framework. *Internet Engineering Task Force (IETF)*, 2012.
- [HFS14] Marian Harbach, Sascha Fahl, and Matthew Smith. Who’s afraid of which bad wolf? a survey of it security risk awareness. In *IEEE 27th CSF*, 2014.
- [HJR15] Marit Hansen, Meiko Jensen, and Martin Rost. Protection goals for privacy engineering. In *IEEE Security and Privacy Workshops*, pages 159–166, 2015.

- [HK16] Gary Hsieh and Rafał Kocielnik. You get who you pay for: The impact of incentives on participation bias. In *Proceedings of the 19th ACM conference on computer-supported cooperative work & social computing*, pages 823–835, 2016.
- [Hoe14] Jaap-Henk Hoepman. Privacy design strategies. In *IFIP International Information Security Conference*, pages 446–459. Springer, 2014.
- [Hoe18] J-H Hoepman. *Privacy Design Strategies (The Little Blue Book)*. Nijmegen: Radboud University, 2018.
- [Hof19] Xenia Hofmeier. Formal analysis of web single-sign on protocols using tamarin. 2019.
- [HPL12] Dick Hardt, Aaron Parecki, and Torsten Lodderstedt. The oauth 2.1 authorization framework draft-parecki-oauth-v2-1-03. *Internet Engineering Task Force (IETF)*, 2012.
- [HSB20] Sven Hammann, Ralf Sasse, and David Basin. Privacy-preserving openid connect. In *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*, pages 277–289, 2020.
- [IC10] Information and Privacy Commissioner/Ontario and Ann Cavoukian. *Privacy Risk Management: Building privacy protection into a Risk Management Framework to ensure that privacy risks are managed, by default*. Information and Privacy Commissioner/Ontario, 2010.
- [ICO] ICO (Information Commission’s Office). Data protection self assessment. <https://ico.org.uk/for-organisations/data-protection-self-assessment/>. Accessed: 2020-02-25.
- [ICO14] ICO (Information Commission’s Office). Conducting privacy impact assessments code of practice. <https://www.pdpjournals.com/docs/88317.pdf>, 2014. Accessed: 2019-19-06.
- [ICO18] ICO (Information Commission’s Office). Data protection impact assessments. <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias-1-0.pdf>, 2018. Accessed: 2019-19-06.
- [ID18] Internet-Draft. International Government Assurance Profile (iGov) for OpenID Connect 1.0, 2018.

- [JBS15] Michael Jones, John Bradley, and Nat Sakimura. Json web token (jwt). *Internet Engineering Task Force (IETF)*, 2015.
- [JKN⁺20] Abdul Bashiru Jibril, Michael Adu Kwarteng, Fortune Nwaiwu, Christina Appiah-Nimo, Michal Pilik, and Miloslava Chovancova. On-line identity theft on consumer purchase intention: A mediating role of online security and privacy concern. In *I3E*. Springer, 2020.
- [KK12] Hanna Krasnova and Paula Kift. Online privacy concerns and legal assurance: a user perspective. In *AIS SIGSEC WISP*, 2012.
- [KKVG11] Ksenia Koroleva, Hanna Krasnova, Natasha F Veltri, and Oliver Günther. It’s all about networking! Empirical investigation of social capital formation on social network sites. *Proceedings of the 32nd ICIS*, 2011.
- [Kob01] Alfred Kobsa. Tailoring privacy to users’ needs. In *ACM UMAP*. Springer, 2001.
- [Kre] Brian Krebs. Internet bank account takeover of +1m users without user interaction. <https://mrbriankrebs.medium.com/internet-bank-account-takeover-of-1m-users-without-user-interaction-4fc9141740a3>. Accessed: 2021-03-25.
- [KTTV17] Sabrina Karwatzki, Manuel Trenz, Virpi Kristiina Tuunainen, and Daniel Veit. Adverse consequences of access to individuals’ information: an analysis of perceptions and the scope of organisational influence. *EJIS*, 26, 2017.
- [Kur00] Karen S Kurasaki. Intercoder reliability for validating conclusions drawn from open-ended interview data. *Field methods*, 12, 2000.
- [KVG12] Hanna Krasnova, Natasha F Veltri, and Oliver Günther. Self-disclosure and privacy calculus on social networking sites: The role of culture. *BISE*, 4, 2012.
- [LB12] Daniel LeBlanc and Robert Biddle. Risk perception of internet-related activities. In *PST*. IEEE, 2012.
- [LBLF20] Torsten Lodderstedt, John Bradley, Andrey Labunets, and Daniel Fett. OAuth 2.0 Security Best Current Practice (draft-ietf-oauth-security-topics-16). *Internet Engineering Task Force (IETF)*, 2020.

- [LBW08] Heather Richter Lipford, Andrew Besmer, and Jason Watson. Understanding privacy settings in Facebook with an audience view. *UPSEC*, 8, 2008.
- [LHP⁺19] Oliver Lipps, Jessica ME Herzing, Nicolas Pekari, Michèle Ernst Stähli, Alexandre Pollien, Gisana Riedo, and Maud Reveilhac. Incentives in surveys. Technical report, FORS, University of Lausanne, 2019.
- [LLR05] Saadi Lahlou, Marc Langheinrich, and Carsten Röcker. Privacy and trust issues with invisible computers. *CACM*, 48, 2005.
- [LM20] Wanpeng Li and Chris J Mitchell. User access privacy in oauth 2.0 and openid connect. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 664–6732. IEEE, 2020.
- [LMD03] Scott Lederer, Jennifer Mankoff, and Anind K Dey. Who wants to know what when? privacy preference determinants in ubiquitous computing. In *CHI’03*, pages 724–725, 2003.
- [LMH13] Torsten Lodderstedt, M McGloin, and P Hunt. Rfc 6819: Oauth 2.0 threat model and security considerations. *Internet Engineering Task Force (IETF)*, pages 1–71, 2013.
- [LMW10] Mikhail A Lisovich, Deirdre K Mulligan, and Stephen B Wicker. Inferring personal information from demand-response systems. *IEEE Security & Privacy*, 8(1), 2010.
- [LSS10] Mass Soldal Lund, Bjørnar Solhaug, and Ketil Stølen. *Model-driven risk analysis: the CORAS approach*. Springer Science & Business Media, 2010.
- [MDMÖG18] Itishree Mohallick, Katrien De Moor, Özlem Özgöbek, and Jon Atle Gulla. Towards new privacy regulations in Europe: Users’ privacy perception in recommender systems. In *SpaCCS*. Springer, 2018.
- [MH15] Rene Meis and Maritta Heisel. Supporting privacy impact assessments using problem-based privacy analysis. In *ICSOFT*, pages 79–98. Springer, 2015.
- [NB19] Jorge Navas and Marta Beltrán. Understanding and mitigating openid connect threats. *Computers & Security*, 84:1–16, 2019.

- [NHH07] Patricia A Norberg, Daniel R Horne, and David A Horne. The privacy paradox: Personal information disclosure intentions versus behaviors. *JCA*, 41, 2007.
- [NIS] NISTIR. Nist privacy risk assessment methodology (PRAM). <https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources>. Accessed: 2021-03-01.
- [NIS08] NIST (National Institute of Standard and Technology). Volume I: Guide for mapping types of information and information systems to security categories. special publication 800-60. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf>, 2008.
- [Nis09] Helen Nissenbaum. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press, 2009.
- [NIS13] NIST (National Institute of Standard and Technology). Security and privacy controls for federal information systems and organization. special publication 800-53. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>, 2013.
- [NIS20] NIST (National Institute of Standard and Technology). The NIST privacy framework: A tool for improving privacy through enterprise risk management. <https://www.nist.gov/privacy-framework/privacy-framework>, 2020.
- [oAIC14] Office of Australian Information Commissioner. Guide to undertaking privacy impact assessments. <https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/>, 2014.
- [OGH05] Judith S Olson, Jonathan Grudin, and Eric Horvitz. A study of preferences for sharing and privacy. In *CHI'05*, 2005.
- [OL08] Isabelle Oomen and Ronald Leenes. Privacy risk perceptions and privacy protection strategies. In *Policies and research in identity management*. Springer, 2008.
- [oMB16] Office of Management and Budget. Circular no. a-130: Managing information as a strategic resource. <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf>, 2016. Accessed: 2021-02-23.

- [OMGMR⁺10] Roberto Ortiz, Santiago Moral-García, Santiago Moral-Rubio, Belén Vela, Javier Garzás, and Eduardo Fernández-Medina. Applicability of security patterns. In *OTM Confederated International Conferences" On the Move to Meaningful Internet Systems"*, pages 672–684. Springer, 2010.
- [Ope] OpenID Foundation. Financial-grade API - part 1: Baseline security profile. <https://openid.net/certification/>. Accessed: 2020-23-11.
- [OS14] Marie Caroline Oetzel and Sarah Spiekermann. A systematic methodology for privacy impact assessments: a design science approach. *European Journal of Information Systems*, 23(2):126–150, 2014.
- [OSG⁺11] Marie Caroline Oetzel, Sarah Spiekermann, Ingrid Grüning, Harald Kelter, and Sabine Mull. Privacy impact assessment guideline for RFID applications. *Federal Office for Information Security (BSI), Germany*, 2011.
- [Paj14] Elda Paja. *STS: a Security Requirements Engineering methodology for socio-technical Systems*. PhD thesis, University of Trento, 2014.
- [Pep14] Scott R Peppet. Regulating the internet of things: first steps toward managing discrimination, privacy, security and consent. *Tex. L. Rev.*, 93:85, 2014.
- [Pet08] John Sören Pettersson. Hci guidelines. *PRIME deliverable D, 6*, 2008.
- [PM12] Andreas Pashalidis and Chris J Mitchell. Privacy in identity and access management systems. In *Digital Identity and Access Management: Technologies and Frameworks*, pages 316–328. IGI Global, 2012.
- [PPHR20] Shani Pitcho-Prelourentzos, Christian Heckel, and Lia Ring. Predictors of social anxiety among online dating users. *COHB*, page 106381, 2020.
- [Pre13] Sören Preibusch. Guide to measuring privacy concern: Review of survey and observational instruments. *International Journal of Human-Computer Studies*, 71, 2013.
- [Rad14] Emilee Rader. Awareness of behavioral tracking and information privacy concern in Facebook and Google. In *10th Symposium On SOUPS*, 2014.

- [raw] Surveys' raw data. <https://www.dropbox.com/scl/fi/myshh9om8ituqv3qoeh9r/GuidedSurvey-BePublished.xlsx?dl=0&rlkey=ysgln6mhnqfukmuqmanmf3i6n>.
- [RB11] Martin Rost and Kirsten Bock. Privacy by design and the new protection goals. *Datenschutz und Datensicherheit*, pages 1–9, 2011.
- [RD16] Lee Rainie and Maeve Duggan. Privacy and information sharing. *Pew Research Center*, 16, 2016.
- [Riv19] Giovanni Maria Riva. Privacy architecting of GDPR-compliant high-tech systems: the PAGHS methodology. Master's thesis, University of Twente, 2019.
- [RJ18] Justin Richer and Leif Johansson. Vector of trust (rfc 8485). *IETF (Internet Engineering Task Force)*, 2018.
- [RP09] Martin Rost and Andreas Pfitzmann. Datenschutzschutzziele—revisited. *Datenschutz und Datensicherheit*, 33(6):353–358, 2009.
- [RS17] Silvio Ranise and Hari Siswantoro. Automated legal compliance checking by security policy analysis. In *International Conference on Computer Safety, Reliability, and Security*, pages 361–372. Springer, 2017.
- [Sak] Nat Sakimura. Authorization delegation: A financial accounts aggregation use case. <https://nat.sakimura.org/2016/01/29/authorization-delegation-a-financial-accounts-aggregation-use-case/>. Accessed: 2021-03-25.
- [SB12] San-Tsai Sun and Konstantin Beznosov. The devil is in the (implementation) details: an empirical analysis of oauth sso systems. In *Proceedings of ACM conference on Computer and communications security*, pages 378–390, 2012.
- [SBA15] Nat Sakimura, John Bradley, and Naveen Agarwal. Proof key for code exchange by oauth public clients. *Internet Engineering Task Force (IETF)*, 2015.
- [SBJ] Nat Sakimura, John Bradley, and Edmund Jay. Financial-grade api - part 1: Baseline security profile. Accessed: 2020-23-11.

- [SBJ⁺14] Nat Sakimura, John Bradley, Mike Jones, Breno De Medeiros, and Chuck Mortimore. OpenID connect core 1.0 incorporating errata set 1. *The OpenID Foundation, specification*, 335, 2014.
- [SC08] Sarah Spiekermann and Lorrie Faith Cranor. Engineering privacy. *Transactions on software engineering*, 35(1):67–82, 2008.
- [Sch06] Bruce Schneier. *Beyond fear: Thinking sensibly about security in an uncertain world*. Springer Science & Business Media, 2006.
- [SCRS19] Amir Sharif, Roberto Carbone, Silvio Ranise, and Giada Sciarretta. A wizard-based approach for secure code generation of single sign-on and access delegation solutions for mobile native apps. In *16th International Joint Conference on e-Business and Telecommunications-SECRYPT*, volume 2, pages 268–275, 2019.
- [SDX11] H Jeff Smith, Tamara Dinev, and Heng Xu. Information privacy research: an interdisciplinary review. *MIS quarterly*, 2011.
- [Sim] Similartech.com. Login providers. <https://www.similartech.com/categories/login-provider>. Accessed: 2020-29-12.
- [SMS14] Alberto Siena, Mirko Morandini, and Angelo Susi. Modelling risks in open source software component selection. In *International Conference on Conceptual Modeling*, pages 335–348. Springer, 2014.
- [SO14] Sarah Spiekermann and Marie Caroline Oetzel. A systematic methodology for privacy impact assessments: a design science approach. *European Journal of Information Systems*, 23(2):128–150, 2014.
- [Sol05] Daniel J Solove. A taxonomy of privacy. *University of Pennsylvania Law Review*, 154:477, 2005.
- [Sol08] Daniel J Solove. *Understanding privacy*. Harvard University Press, 2008.
- [Sol20] Daniel J Solove. The myth of the privacy paradox. *Available at SSRN*, 2020.
- [Spe11] Special Eurobarometer 359. Attitudes on data protection and electronic identity in the European Union, 2011.
- [Spe15] Special Eurobarometer 431. Data protection, 2015.
- [Spe19] Special Eurobarometer 487a. 87a. general data protection regulation, 2019.

- [Spi12] Sarah Spiekermann. The RFID PIA—developed by industry, endorsed by regulators. In David Wright and Paul de Hert, editors, *Privacy impact assessment*, chapter 15, pages 323–346. Springer, 2012.
- [Sta69] Chauncey Starr. Social benefit versus technological risk. *Science*, 1969.
- [Sup] European Data Protection Supervisor. Necessity and proportionality. https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en. Accessed: 2020-01-03.
- [SV14] Fatemeh Shirazi and Melanie Volkamer. What deters jane from preventing identification and tracking on the web? In *Proceedings of the WPES*, 2014.
- [SWB⁺12] J Sabo, M Willett, P Brown, G Janssen, and DN Jutla. Privacy management reference model and methodology (PMRM) version 1.0. *OASIS Open*, 2012.
- [SWBS19] Wolfgang Schulz, Florian Wittner, Kai Bavendiek, and Sibylle Schupp. Modeling and verification in GDPR’s data protection impact assessment. <https://www.cdpconferences.org/archive>, 2019.
- [SWS07] Anoop Singhal, Theodore Winograd, and Karen Scarfone. Guide to secure web services. *NIST Special Publication*, 800(95):4, 2007.
- [SYF18] Michael Warren Skirpan, Tom Yeh, and Casey Fiesler. What’s at stake: Characterizing risk perceptions of emerging technologies. In *Proceedings of CHI*, 2018.
- [TD] Lodderstedt Torsten and Fett Daniel. Openid connect for identity assurance 1.0. https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html. Accessed: 2019-19-06.
- [TdHRZ17] Fatih Turkmen, Jerry den Hartog, Silvio Ranise, and Nicola Zannone. Formal analysis of xacml policies using SMT. *Computers & Security*, 66:185–203, 2017.
- [TM12] Diana I Tamir and Jason P Mitchell. Disclosing information about the self is intrinsically rewarding. *PNAS*, 109, 2012.
- [TSR11] Monique Mitchell Turner, Christine Skubisz, and Rajiv N Rimal. Theory and practice in risk communication: A review of the literature and visions for the future. In *The Routledge handbook of health communication*. Routledge, 2011.

- [TWC12] Eran Toch, Yang Wang, and Lorrie Faith Cranor. Personalization and privacy: a survey of privacy risks and remedies in personalization-based systems. *UMUAI*, 22, 2012.
- [VDGR16] Niels Van Dijk, Raphaël Gellert, and Kjetil Rommetveit. A risk to a right? Beyond data protection risk assessments. *Computer Law & Security Review*, 32(2):286–306, 2016.
- [VK18] Konstantina Vemou and Maria Karyda. An evaluation framework for privacy impact assessment methods. In *12th Mediterranean Conference on Information Systems At: Corfu, Greece*, 2018.
- [vPH17] JPM van Puijenbroek and J-H Hoepman. Privacy impact assessments in practice: Outcome of a descriptive field research in the Netherlands. 2017.
- [VSSJJ06] Craig Van Slyke, JT Shim, Richard Johnson, and James J Jiang. Concern for information privacy and online consumer purchasing. *JAIS*, 7, 2006.
- [VvdB17] Paul Voigt and Axel von dem Bussche. *Practical Implementation of the Requirements Under the GDPR*. In: *The EU General Data Protection Regulation (GDPR)*. Springer, 2017.
- [VZ16] Liesbet Van Zoonen. Privacy concerns in smart cities. *Government Information Quarterly*, 33, 2016.
- [WB90] Samuel D Warren and Louis D Brandeis. The right to privacy. *Harvard law review*, 1890.
- [WdH12] David Wright and Paul de Hert. *Privacy Impact Assessment*, volume 6. Springer Science & Business Media, 2012.
- [Wes67] Alan F Westin. Privacy and freedom atheneum. *New York*, 7, 1967.
- [WFR13] David Wright, Rachel Finn, and Rowena Rodrigues. A comparative analysis of privacy impact assessment in six countries. *JCER*, 9, 2013.
- [WNK⁺11] Yang Wang, Gregory Norcie, Saranga Komanduri, Alessandro Acquisti, Pedro Giovanni Leon, and Lorrie Faith Cranor. “I regretted the minute I pressed share” a qualitative study of regrets on facebook. In *Proceedings of SOUPS*, 2011.
- [WR13] Kush Wadhwa and Rowena Rodrigues. Evaluating privacy impact assessments. *Innovation: The European Journal of Social Science Research*, 26(1-2):161–180, 2013.

- [WRH⁺12] Claes Wohlin, Per Runeson, Martin Höst, Magnus C Ohlsson, Björn Regnell, and Anders Wesslén. *Experimentation in software engineering*. Springer Science & Business Media, 2012.
- [Wri12] David Wright. The state of the art in privacy impact assessment. *Computer law & security review*, 28(1):54–61, 2012.
- [WSJ14] Kim Wuyts, Riccardo Scandariato, and Wouter Joosen. Lind(d)un privacy threat tree catalog. *KU Leuven, Department of Computer Science, Technical Report CW*, 675, 2014.
- [WW16] Jorge Werner and Carla Merkle Westphall. A model for identity management with privacy in the cloud. In *2016 IEEE Symposium on Computers and Communication (ISCC)*, pages 463–468. IEEE, 2016.
- [WW17] Rafael Weingärtner and Carla Merkle Westphall. A design towards personally identifiable information control and awareness in openid connect identity providers. In *2017 IEEE International Conference on Computer and Information Technology (CIT)*, pages 37–46. IEEE, 2017.
- [WXH16] Yang Wang, Huichuan Xia, and Yun Huang. Examining american and chinese internet users’ contextual privacy preferences of behavioral advertising. In *Proceedings of ACM CSCW*, 2016.
- [WXYH16] Yang Wang, Huichuan Xia, Yaxing Yao, and Yun Huang. Flying eyes and hidden controllers: A qualitative study of people’s privacy perceptions of civilian drones in the US. *Proceedings on PET*, 2016.
- [WZ11] Craig E Wills and Mihajlo Zeljkovic. A personalized approach to web privacy: awareness, attitudes and actions. *Inform Manag Comput Secur*, 2011.
- [XM20] Huichuan Xia and Brian McKernan. Privacy in crowdsourcing: a review of the threats and challenges. *Computer Supported Cooperative Work*, 2020.
- [You09] Seounmi Youn. Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *JCA*, 43, 2009.
- [ZJ16] Pei Zhang and Antonie Jetter. Understanding risk perception using fuzzy cognitive maps. In *PICMET*. IEEE, 2016.

- [ZKS⁺20] Zhiyi Zhang, Michał Król, Alberto Sonnino, Lixia Zhang, and Etienne Rivière. El passo: Privacy-preserving, asynchronous single sign-on. *arXiv preprint arXiv:2002.10289*, 2020.
- [ZMR17] Eric Zeng, Shrirang Mare, and Franziska Roesner. End user security and privacy concerns with smart homes. In *13 Symposium on SOUPS*, 2017.
- [ZMW14] Jan Henrik Ziegeldorf, Oscar Garcia Morchon, and Klaus Wehrle. Privacy in the internet of things: threats and challenges. *Security and Communication Networks*, 2014.
- [ZWdH12] Nils Zurawski, David Wright, and Paul de Hert. Privacy impact assessment, springer, 2012, 519 pp, isbn: 978-94-007-2542-3, 2012.

Appendix A

Surveys

This section presents the two surveys.

A.1 The common Parts of the surveys

A.1.1 The First Page

Have you ever experienced receiving ads in different platforms about the trip destination you were googling? Or wondered how social media knows you well enough to suggest things, such as products, news, books, friends, that you like? You use a service which requires you to share some personal data with a purpose in mind, but it is not clear how and what for your data is used later. Sometimes that significantly impacts our lives. Think of how the usage of millions of Facebook user profiles allowed a system to be designed that influenced the results of the US election. In this research, we aim to understand individuals' concerns while using online services. The results of this study will help organizations to estimate better the impact of privacy risks on the private life of individuals and accordingly improve their privacy and security protection. Following, you will be asked to identify your age range. That is to study the relation of age and privacy risks. Then you will be presented a fictional case.

It will be followed by 5 nested categories of risks (e.g., Discrimination/manipulation Concern) each of which contain four privacy risks (e.g., Inaccurate or inappropriate profiling, targeted ads). Given the scenario, you will be asked to estimate the level of impact that privacy risk might have on your private live, in case of a data breach. *(This paragraph goes as following for Unguided survey: Then you are asked to iden-*

tify five privacy risks related to the scenario, the impact they could have on data subjects and possible treatment to counteract.)

The evaluation is on a scale of 1 (negligible) to 4 (maximum), where 1 means that you are not at all concerned and 4 means that you are very concerned. The survey may take up to 10 minutes. (The survey time estimation for *Unguided* and *Pilot Survey* was 20 minutes).

The study can be terminated at any time, without providing reasons and without any negative consequences. Your decision to submit your answer is completely voluntary. However, if you do not submit, it will not be possible for you to participate in the study. There will be no physical safety risks during the study. The responses you enter during the course of the study are recorded. Other than that, no data are collected. The recorded data are evaluated and further processed in the course of the data analysis and published as a scientific paper. It will be impossible to trace the source of the information back to you.

The Second Page **Age Range.** Could you share with us your age range and the continent of your residence?

- ☐ 18- 24
- ☐ 25- 34
- ☐ 35- 44
- ☐ 44- 54
- ☐ 55- 64
- ☐ 65- 74
- ☐ 75 or older

A.1.2 The Third Page

Scenario description. SinTown is a browser-based game, by WickedGammingInc, that allows players to live their craziest intimate fantasies in the virtual world. Users meet in a virtual town with different places, such as clubs and bars, where things happen among two or more players. The game also has private chats and forums where people can connect.

SinTown has more than 8 million users across the globe, and a database of more than 60 Gb of data, including photos, avatars, and chat and forum conversations. Account

creation rate shows thousands of male and female profiles being created every day, thanks to quick subscription method that dismiss email validity verification, and no password format policy to ask for having certain amount of different characters. It also allows user to delete his/her account for which the account will be set inactive in the database, it cannot be deleted completely.

SinTown collects basic information about its users, like name, address, telephone number, gender, date of birth, and credit card number if they want to promote their account to the premium. The premium account has special features like voice and video call.

A.1.3 The Ninth Page

We thank you for participating in the survey.

A.2 Guided Survey: Page 4 to 8

Assess Discrimination/manipulation Risk. *What is your level of concern that the following situations related to discrimination and manipulation may occur as a data breach?*

1. Targeted, unique and nonrecurring, lost opportunities (e.g., refusal of studies, internships or employment, examination ban)

(Negligible) ☐ 1 ☐ 2 ☐ 3 ☐ 4 (Maximum)

2. Feeling of violation of fundamental rights (e.g., discrimination, freedom of expression)

(Negligible) ☐ 1 ☐ 2 ☐ 3 ☐ 4 (Maximum)

3. Targeted online advertising on a private aspect that you want to keep confidential (e.g., pregnancy advertising, drug treatment)

(Negligible) ☐ 1 ☐ 2 ☐ 3 ☐ 4 (Maximum)

4. Inaccurate or inappropriate profiling

(Negligible) ☐ 1 ☐ 2 ☐ 3 ☐ 4 (Maximum)

Assess Financial Risk. *What is your level of concern that the following situations*

related to your personal finances occur as a result of a data breach?

1. Non-temporary financial difficulties

(Negligible) ☐ 1 ☐ 2 ☐ 3 ☐ 4 (Maximum)

2. Unanticipated payment

(Negligible) ☐ 1 ☐ 2 ☐ 3 ☐ 4 (Maximum)

3. Missing career promotion

(Negligible) ☐ 1 ☐ 2 ☐ 3 ☐ 4 (Maximum)

4. Financial loss as a result of a fraud (e.g., after an attempted phishing)

(Negligible) ☐ 1 ☐ 2 ☐ 3 ☐ 4 (Maximum)

Assess Social Disadvantage Risk. *What is your level of concern that the following situations related to your social and personal life may occur as a result of a data breach?*

1. Loss of family tie

(Negligible) ☐ 1 ☐ 2 ☐ 3 ☐ 4 (Maximum)

2. Separation or divorce

(Negligible) ☐ 1 ☐ 2 ☐ 3 ☐ 4 (Maximum)

3. Receipt of unwanted targeted mailings likely to damage your reputation

(Negligible) ☐ 1 ☐ 2 ☐ 3 ☐ 4 (Maximum)

4. Cyberbullying and harassment like blackmailing

(Negligible) ☐ 1 ☐ 2 ☐ 3 ☐ 4 (Maximum)

Assess Deprived to Exercise Your Rights. *What is your level of concern that the following situations related to your personal data rights may occur as a result of data breach?*

1. Losing control over your data

(Negligible) ☐ 1 ☐ 2 ☐ 3 ☐ 4 (Maximum)

2. Reuse of data published on websites for the purpose of targeted advertising (information to social networks, reuse for paper mailing)

(Negligible) ☐ 1 ☐ 2 ☐ 3 ☐ 4 (Maximum)

3. Feeling of invasion of privacy

(Negligible) ☐ 1 ☐ 2 ☐ 3 ☐ 4 (Maximum)

4. Blocked online services account (e.g., games, administration)

(Negligible) ☐ 1 ☐ 2 ☐ 3 ☐ 4 (Maximum)

Assess Physical Risk. *What is your level of concern that the following situations related to your physical and psychological well-being may occur as a result of a data breach?*

1. Psychological problem (e.g., development of a phobia, loss of self-esteem)

(Negligible) ☐ 1 ☐ 2 ☐ 3 ☐ 4 (Maximum)

2. Defamation resulting in physical retaliation

(Negligible) ☐ 1 ☐ 2 ☐ 3 ☐ 4 (Maximum)

3. Physical issues like transient headaches

(Negligible) ☐ 1 ☐ 2 ☐ 3 ☐ 4 (Maximum)

4. Alteration of physical integrity for example following an assault, an accident at home, work, etc

(Negligible) ☐ 1 ☐ 2 ☐ 3 ☐ 4 (Maximum)

A.3 Unguided Survey: Page 4

Privacy Risk 1. Identify a privacy risk related to the scenario in the space below, with an explanation of the impact assessment. _____

Impact estimation:

(Negligible) ☐ 1 ☐ 2 ☐ 3 ☐ 4 (Maximum)

What are the actions or security controls to implement for treating such risk? _____

Privacy Risk 2. Identify a privacy risk related to the scenario in the space below, with an explanation of the impact assessment. _____

Impact estimation:

(Negligible) ☐ 1 ☐ 2 ☐ 3 ☐ 4 (Maximum)

What are the actions or security controls to implement for treating such risk?_____

Privacy Risk 3. Identify a privacy risk related to the scenario in the space below, with an explanation of the impact assessment. _____

Impact estimation:

(Negligible) ☐ 1 ☐ 2 ☐ 3 ☐ 4 (Maximum)

What are the actions or security controls to implement for treating such risk?_____

Privacy Risk 4. Identify a privacy risk related to the scenario in the space below, with an explanation of the impact assessment. _____

Impact estimation:

(Negligible) ☐ 1 ☐ 2 ☐ 3 ☐ 4 (Maximum)

What are the actions or security controls to implement for treating such risk?_____

Privacy Risk 5. Identify a privacy risk related to the scenario in the space below, with an explanation of the impact assessment. _____

Impact estimation:

(Negligible) ☐ 1 ☐ 2 ☐ 3 ☐ 4 (Maximum)

What are the actions or security controls to implement for treating such risk?_____

Appendix B

NIST Catalog of Problematic Data Actions and Problems

This section represents the *Catalog of Problematic Data Actions and Problems* introduced in [\[NIS\]](#).

B.1 Problematic Data Actions

- **Appropriation:** Data is used in ways that exceed an individual's expectation or authorization (e.g., implicit or explicit). Appropriation includes scenarios in which the individual would have expected additional value for the use given more complete information or negotiating power. Privacy problems that appropriation can lead to include loss of trust, loss of autonomy, and economic loss.
- **Distortion:** Inaccurate or misleadingly incomplete data is used or disseminated. Distortion can present users in an inaccurate, unflattering, or disparaging manner, opening the door for stigmatization, discrimination, or loss of liberty.
- **Induced Disclosure:** Induced disclosure can occur when individuals feel compelled to provide information disproportionate to the purpose or outcome of the transaction. Induced disclosure can include leveraging access or rights to an essential (or perceived essential) service. It can lead to problems such as discrimination, loss of trust, or loss of autonomy.

- **Insecurity:** Lapses in data security can result in various problems, including loss of trust, exposure to economic loss and other identity theft-related harms, and dignity losses.
- **Re-identification:** De-identified data, or data otherwise disassociated from specific individuals, becomes identifiable or associated with specific individuals again. It can lead to problems such as discrimination, loss of trust, or dignity losses.
- **Stigmatization:** Data is linked to an actual identity in such a way as to create a stigma that can cause dignity losses or discrimination. For example, transactional or behavioral data such as the accessing of certain services (e.g., food stamps or unemployment benefits) or locations (e.g., health care providers) may create inferences about individuals that can cause dignity losses or discrimination.
- **Surveillance:** Data, devices or individuals are tracked or monitored in a manner disproportionate to the purpose. The difference between a benign action and the problematic data action of surveillance can be narrow. Tracking or monitoring may be conducted for operational purposes such as cybersecurity or to provide better services, but it can become surveillance when it leads to problems such as discrimination; loss of trust, autonomy, or liberty; or physical harm.
- **Unanticipated Revelation:** Data reveals or exposes an individual or facets of an individual in unexpected ways. Unanticipated revelation can arise from aggregation and analysis of large and/or diverse data sets. Unanticipated revelation can give rise to dignity losses, discrimination, and loss of trust and autonomy.
- **Unwarranted Restriction:** Unwarranted restriction includes not only blocking access to data or services, but also limiting awareness of the existence of data or its uses in ways that are disproportionate to operational purposes. Operational purposes may include fraud detection or other compliance processes. When individuals do not know what data an entity has or can make use of, they do not have the opportunity to participate in decision-making. Unwarranted restriction also diminishes accountability as to whether the data is appropriate for the entity to possess or it will be used in a fair or equitable manner. Lack of access to data or services can lead to problems in the loss of self-determination category, loss of trust, and economic harm.

B.2 Problems

- **Dignity Loss:** Includes embarrassment and emotional distress
- **Discrimination:** Unfair or unethical differential treatment of individuals whether singly or as a group arising from the processing of data.
- **Economic Loss:** Can include direct financial losses as the result of identity theft or the failure to receive fair value in a transaction.
- **Loss of Self Determination**
 - **Loss of Autonomy:** Includes losing control over determinations about information processing or interactions with systems/products/services, as well as needless changes in ordinary behavior, including self-imposed restrictions on expression or civic engagement.
 - **Loss of Liberty:** Incomplete or inaccurate data can lead to improper exposure to arrest or detainment. Improper exposure or use of information can contribute to abuses of governmental power.
 - **Physical Harm:** Physical harm or death.
- **Loss of Trust:** The breach of implicit or explicit expectations or agreements about the processing of data. These breaches can diminish morale or leave individuals reluctant to engage in further transactions potentially creating larger economic or civic consequences.

B.3 Related Privacy Enhanced Technologies to Privacy Goals

The following table lists design solutions and practical advises introduced in [SO14, DWS⁺11, BEL17].

	[DWS+11]	[BEL17]	[SO14]
lawfulness, fairness and transparency	Policy communication (P3P), Policy enforcement (XACML,EPAL), Feedback tools for user privacy awareness, Data removal tools (spyware removal, browser cleaning tools, activity traces eraser, harddisk data eraser)	Embedded transparency measure: embedding necessary forms, dialogues, notifications into information system. Such as asking for consent before collecting location data of a mobile app user. Embedded legal measures: for example, an embedded database that capture consents from users of the information system and map it to the user data. tis can help the users to exercise their rights and the organization to manage their obligations. Non-repudiation service: implementing the non-repudiation service from the data subjects. for example, the digital signature shall be implemented when the collected data is sensitive.	Providing accurate and up-to date information. Making information accessible, providing a privacy statement, ensuring obtaining of consent, checking validity of consent, providing adequate information in cases of direct and indirect collection of data from data subject, providing an interface that allows data subjects to send in a request for information, ensuring timely processing of data subjects' request for information, providing accurate and up-to-date information concerning (a) confirmation as to whether or not data relating to the data subject if being processed, (b) the purpose of the processing, (c) the data undergoing processing and any information as to data's source, (f) the logic involved in any automatic processing of data and automated decisions.
purpose limitation		Data inventory: functionality to trace back the purpose of the data collection, this can be achieved by adding meta-data or tagging to the personal data, this can be linked to the data minimization and storage limitation purpose. Reporting: automatic notification and reporting functionality embedded into the information systems.	ensuring legitimacy of purpose, ensuring purpose related processing through policies and regular audits, authentication, authorization, logging, providing an accurate and up-to-date purpose specification
Interveinability			authenitcation, authorization, logging, export functionality, providing adequate and timely information about rectification, erasure and blocking of data to relevant third parties, providing and intrface that allows data subjects to send in an objection, ensuring timely processing of data subject's objection

Data minimization	Centralized storage: limiting the disturb of storing personal data in distributed environment and consolidate the personal data in central storage can contribute to data minimization. Data pseudonymization: encrypting some of the data fields that can link the data persons, such as name, birthdays, address. keys should be handled carefully to prevent recovering the encrypted fields. Strip unused meta data: files documents, videos can contain personal data about the author, the geographic location of the user and IP address that may not be necessary for the data processing. Cleaning these meta data might be necessary. Intermediary proxies: data collection and data transmission through intermediary proxies to filter and anonymize personal data such as IP address, and cookies.	pseudonymization, anonymization, obfuscation, automated deletion routines, ensuring data minimization through policies and regular audits, provide and enforcing deletion rules
accuracy	Input validation validate all inputs to information system, and allow only valid data and formats to the system. For example, allow only UK data format. Data dispute handling: functionalities to notify data subjects about any changes to personal data in the information systems, and measures to allow data subjects objects or report any issue about their personal data processed in the systems. Data cleansing: functionalities to analyze the correctness and consistency of personal data in information systems and deleted inaccurate or incomplete data.	data validation
storage limitation	Traceability: functionality in the information system that can report and visualize the route the actual data to the backup, and or other distributed copies. This can enable organization to remove unnecessary data. Self wiping: for example, an embedded database that capture consents from users of the information system and map it to the user data. this can help the users to exercise their rights and the organization to manage their obligations. Reporting: implementing the non-repudiation services from the data subjects. for example, the digital signature shall be implemented when the collected data in sensitive	automated deletion routines, providing and enforcing deletion rules

accountability	DC-net & MIX-net + dummy traffic, ISDN-mixes, Broadcast systems + dummy traffic	Authentication and authorization embedding necessary forms, dialogues, notifications into information system. Such as asking for consent before collecting location data of a mobile app user. Tamper proof audit trails: information system should provide audit logs that can be used for monitoring compliance, and any future investigation or reporting. tamper proof audits trail be implemented strictly in IT systems.]Monitoring: the goal with privacy should be always to prevent data leakage. although monitoring be a re-active approach, but it can help the organization on prevent future incidents. Data loss prevention preventing data from leakage on the way out from information systems or organizations considered to be one of the important functions for data protection.	authentication, authorization, logging
integrity and confidentiality	ISDN-mixes, Onion Routing , Crowds, Single proxy (Penet pseudonymous remailer, Anonymizer, SafeWeb), anonymous Remailer (Cipherpunk Type 0, Type 1 , Mixmaster Type 2, Mixminion Type 3), and Low-latency communication , Java Anon Proxy (JAP), Tor,DC-net & MIX-net + dummy traffic, Broadcast systems, Private authentication, Anonymous credentials (single show, multitown) Deniable authentication, Off-the-record messaging, Privacy preserving cryptographic protocols, Multi-party computation,Anonymous buyer-seller watermarking protocol, Information retrieval Private information retrieval + dummy traffic, Oblivious transfer]), Privacy preserving data mining, Searchable encryption, Private search, Data anonymization K-anonymity model, l-Diversity, Information hiding Steganography, Covert communication, Spread spectrum, Pseudonymity systems Privacy enhancing identity management system, User-controlled identity management system, Privacy preserving biometrics, Encryption techniques Symmetric key & public key encryption, Deniable encryption, Homomorphic encryption, Verifiable encryption, Access control techniques	End to end encryption: encryption personal data at rest, in transit and in use when possible, depending on the sensitivity of personal data. Other techniques such as anonymization and pseudonymization can achieve the same objective. Data validation: adequate level of authentication depending on the level of risk based on principle/ combination of two can be necessary for Special category processing. Authorization: access rights management by using models such as role based on any other models to ensure data always kept secret and prevent the risk of disclosure of personal data to unauthorized invalidation.	technical information security controls, administrative/managerial information security controls, providing adequate and timely information about personal data breach to data subject

Appendix C

The Questionnaires

C.1 Control Questionnaire

Following Listing C.1 represents the output of the *Control Questionnaire*. Note that, we have omitted the controls whose answer was 'NO'.

Listing C.1: Controls Questionnaire responses

```
1 {
2   "Confidentiality":
3     [{
4       "SecurityControl": "Identification and authentication" ,
5       "Identifier": "IA-2",
6       "baseline": [{"Low":["IA-2"]},
7                   {"Moderate":["IA-2"]},
8                   {"High":["IA-2", "IA-3", "IA-4", "IA-8"]}],
9       "question": "Do you provide any Identification and authentication?",
10      "Answer": "Yes",
11      "SecurityTechVendor": "Auth0",
12      "SecurityTechProduct": "Auth0.js",
13      "SecurityTechVersion": "8.10.1",
14      "OtherGoal": ["Integrity"]
15    },
16    {
17      "SecurityControl": "Authenticator feedback" ,
18      "Identifier": "IA-6",
19      "baseline": [{"Low":["IA-6"]},
```

```

20         {"Moderate":["IA-6"]},
21         {"High":["IA-6"]}],
22     "question":"Do you obscure the authentication feedback?",
23     "Answer": "Yes",
24     "SecurityTechVendor": "Auth0",
25     "SecurityTechProduct": "Auth0.js",
26     "SecurityTechVersion": "8.10.1",
27     "OtherGoal":["Integrity]
28 },
29 { "SecurityControl": "Access enforcement",
30   "Identifier": "AC-3",
31   "baseline": [{"Low":["AC-3"]},
32               {"Moderate":["AC-3"]},
33               {"High":["AC-3"]}],
34   "question":"Do you provide any Access enforcement?",
35   "Answer": "Yes",
36   "SecurityTechVendor": "Microsoft",
37   "SecurityTechProduct": "Active Directory Federation Services",
38   "SecurityTechVersion": "4.0",
39   "OtherGoal":["Integrity"]
40 },
41   { "SecurityControl": "Account management",
42     "Identifier": "AC-2",
43     "baseline": [{"Low":["AC-2"]},
44                 {"Moderate":["AC-2", "AC-3", "AC-4"]},
45                 {"High":["AC-2", "AC-3", "AC-4", "AC-5", "AC-11", "AC-12"]}],
46     "question":"Do you provide any account management?",
47     "Answer": "Yes",
48     "SecurityTechVendor": "Microsoft",
49     "SecurityTechProduct": "Active Directory Federation Services",
50     "SecurityTechVersion": "4.0",
51     "OtherGoal":["Integrity"]
52 },
53 { "SecurityControl": "Least privilege",
54   "Identifier": "AC-6",
55   "baseline": [{"Low":[]},
56               {"Moderate":["AC-2", "AC-5", "AC-9", "AC-10"]},
57               {"High":["AC-2", "AC-3", "AC-5", "AC-9", "AC-10"]}],
58   "question":"Do you apply Least privilege strategies?",
59   "Answer": "Yes",
60   "SecurityTechVendor": "Microsoft",

```

```

61 "SecurityTechProduct": "Active Directory Federation Services",
62 "SecurityTechVersion": "4.0",
63 "OtherGoal":["Integrity"]
64 },
65 { "SecurityControl": "Session lock",
66 "Identifier": "AC-11",
67 "baseline": [{"Low":[]},
68             {"Moderate":["AC-11"]},
69             {"High":["AC-11"]}],
70 "question":"Have you configured Session lock?",
71 "Answer": "Yes",
72 "SecurityTechVendor": "",
73 "SecurityTechProduct": "",
74 "SecurityTechVersion": "",
75 "OtherGoal":["Integrity"]
76 },
77 { "SecurityControl": "Session termination",
78 "Identifier": "AC-12",
79 "baseline": [{"Low":[]},
80             {"Moderate":["AC-12"]},
81             {"High":["AC-12"]}],
82 "question":"Have you configured Session termination?",
83 "Answer": "Yes",
84 "SecurityTechVendor": "",
85 "SecurityTechProduct": "",
86 "SecurityTechVersion": "",
87 "OtherGoal":["Integrity"]
88 },
89 { "SecurityControl": "Remote Access",
90 "Identifier": "AC-17",
91 "baseline": [{"Low":["AC-17"]},
92             {"Moderate":["AC-17", "AC-2", "AC-3", "AC-4"]},
93             {"High":["AC-17", "AC-2", "AC-3", "AC-4"]}],
94 "question":"Have you protected remote access to the information system?",
95 "Answer": "Yes",
96 "SecurityTechVendor": "PulseSecure",
97 "SecurityTechProduct": "Pulse Connect Secure",
98 "SecurityTechVersion": "43",
99 "OtherGoal":["Integrity"]
100 },
101 { "SecurityControl": "Identifier management",

```

```

102 "Identifier": "IA-4",
103 "baseline": [{"Low":["IA-4"]},
104             {"Moderate":["IA-4"]},
105             {"High":["IA-4"]}],
106 "question":"Do you provide any Identifier management?",
107 "Answer": "Yes",
108 "SecurityTechVendor": "Microsoft",
109 "SecurityTechProduct": "Active Directory Federation Services",
110 "SecurityTechVersion": "4.0",
111 "OtherGoal":["Integrity"]
112 },
113 { "SecurityControl": "Authenticator management",
114 "Identifier": "IA-5",
115 "baseline": [{"Low":["IA-5"]},
116             {"Moderate":["IA-5", "IA-2", "IA-3"]},
117             {"High":["IA-4"]}],
118 "question":"Do you provide any Authenticator management?",
119 "Answer": "Yes",
120 "SecurityTechVendor": "Microsoft",
121 "SecurityTechProduct": "Active Directory Federation Services",
122 "SecurityTechVersion": "4.0",
123 "OtherGoal":["Integrity"]
124 },
125 { "SecurityControl": "Identification and authentication (non-organizational
    users)",
126 "Identifier": "IA-8",
127 "baseline": [{"Low":["IA-8"]},
128             {"Moderate":["IA-8", "IA-4", "IA-2", "IA-3"]},
129             {"High":["IA-8", "IA-4", "IA-2", "IA-3"]}],
130 "question":"Do you provide any Identification and authentication (non-
    organizational users)?",
131 "Answer": "Yes",
132 "SecurityTechVendor": "ownCloud",
133 "SecurityTechProduct": "ownCloud Server",
134 "SecurityTechVersion": "10.0.1",
135 "OtherGoal":["Integrity"]
136 },
137 { "SecurityControl": "Application partitioning",
138 "Identifier": "SC-2",
139 "baseline": [{"Low":[]},
140             {"Moderate":["SC-2"]},

```

```

141         {"High":["SC-2"]}],
142         "question":"Do you separate user functionality from information system
management functionality?",
143         "Answer": "Yes",
144         "SecurityTechVendor": "Microsoft",
145         "SecurityTechProduct": "Active Directory Federation Services",
146         "SecurityTechVersion": "4.0",
147         "OtherGoal":["Integrity"]
148     },
149     {
150         "SecurityControl": "Transmission confidentiality and integrity",
151         "Identifier": "SC-8",
152         "baseline": [{ "Low":[]},
153             {"Moderate":["SC-8"]},
154             {"High":["SC-8"]}],
155         "question":"Do you secure the communication channel?",
156         "Answer": "Yes",
157         "SecurityTechVendor": "Cisco",
158         "SecurityTechProduct": "firepower management center",
159         "SecurityTechVersion": "6.4.0",
160         "OtherGoal":["Integrity"]
161     },
162     { "SecurityControl": "Unsuccessful logon attempts",
163         "Identifier": "AC-7",
164         "baseline": [{ "Low":["AC-7"]},
165             {"Moderate":["AC-7"]},
166             {"High":["AC-7"]}],
167         "question":"Do you handle Unsuccessful logon attempts?",
168         "Answer": "Yes",
169         "SecurityTechVendor": "Microsoft",
170         "SecurityTechProduct": "Active Directory Federation Services",
171         "SecurityTechVersion": "4.0",
172         "OtherGoal":["Integrity"]
173     },
174     { "SecurityControl": "Information in shared resources",
175         "Identifier": "SC-4",
176         "baseline": [{ "Low":["SC-4"]},
177             {"Moderate":["SC-4"]},
178             {"High":["SC-4"]}],
179         "question":"Do you provide any Information in shared resources?",
180         "Answer": "Yes",

```

```

181 "SecurityTechVendor": "ownCloud",
182 "SecurityTechProduct": "ownCloud Server",
183 "SecurityTechVersion": "10.0.1",
184 "OtherGoal": []
185 },
186 { "SecurityControl": "Information sharing",
187 "Identifier": "AC-21",
188 "baseline": [{"Low": []},
189               {"Moderate": ["AC-21"]},
190               {"High": ["AC-21"]}],
191 "question": "Do you provide any restriction to access shared Information
192 ?" ,
193 "Answer": "Yes",
194 "SecurityTechVendor": "ownCloud",
195 "SecurityTechProduct": "ownCloud Server",
196 "SecurityTechVersion": "10.0.1",
197 "OtherGoal": ["Integrity"]
198 },
199 { "SecurityControl": "Protection of information at rest",
200 "Identifier": "SC-28",
201 "baseline": [{"Low": []},
202               {"Moderate": ["SC-28"]},
203               {"High": ["SC-28"]}],
204 "question": "Do you provide any protection for information at rest?",
205 "Answer": "Yes",
206 "SecurityTechVendor": "ownCloud",
207 "SecurityTechProduct": "ownCloud Server",
208 "SecurityTechVersion": "10.0.1",
209 "OtherGoal": ["Integrity"]
210 },
211 { "SecurityControl": "Boundary protection",
212 "Identifier": "SC-7",
213 "baseline": [{"Low": ["SC-7"]},
214               {"Moderate": ["SC-3", "SC-4", "SC-5", "SC-7"]},
215               {"High": ["SC-3", "SC-4", "SC-5", "SC-7", "SC-8", "SC-18"]}],
216 "question": "Do you provide any Boundary protection?",
217 "Answer": "Yes",
218 "SecurityTechVendor": "Juniper Networks",
219 "SecurityTechProduct": "Junos Space",
220 "SecurityTechVersion": "15.2",
221 "OtherGoal": "Availability"

```

```

221 },
222 { // We have put the following control by its family as
223   // the answer to all its memeber were Not applicable.
224   "SecurityControl": "Media protection",
225   "Identifier": "MP",
226   "question": "Do you provide any media protection?",
227   "Answer": "Not Applicable",
228   "SecurityTechVendor": "",
229   "SecurityTechProduct": "",
230   "SecurityTechVersion": "",
231   "OtherGoal": ["Integrity"]
232 }
233 ],
234 "Integrity":
235 [{"SecurityControl": "Information handling and retention",
236   "Identifier": "SI-12",
237   "baseline": [{"Low": ["SI-12"]},
238     {"Moderate": ["SI-12"]},
239     {"High": ["SI-12"]}],
240   "question": "Do you provide any Information handling and retention?",
241   "Answer": "Yes",
242   "SecurityTechVendor": "ownCloud",
243   "SecurityTechProduct": "ownCloud Server",
244   "SecurityTechVersion": "10.0.1",
245   "OtherGoal": []
246 }],
247 {"SecurityControl": "Software, firmware, and information integrity",
248   "Identifier": "SI-7",
249   "baseline": [{"Low": []},
250     {"Moderate": ["SI-7"]},
251     {"High": ["SI-7"]}],
252   "question": "Do you satitfy Software, firmware, and information integrity
253   ?",
254   "Answer": "Yes",
255   "SecurityTechVendor": "Microsoft",
256   "SecurityTechProduct": "Azure Security center",
257   "SecurityTechVersion": "",
258   "OtherGoal": []
259 },
260 {"SecurityControl": "Spam protection",

```

```

261 "Identifier": "SI-8",
262 "baseline": [{"Low": []},
263             {"Moderate": ["SI-2", "SI-8"]},
264             {"High": ["SI-8", "SI-2"]}],
265 "question": "Do you protect system from spam?",
266 "Answer": "Yes",
267 "SecurityTechVendor": "Microsoft",
268 "SecurityTechProduct": "Azure Security center",
269 "SecurityTechVersion": "",
270 "OtherGoal": []
271 },
272 {
273 "SecurityControl": "Malicious code protection",
274 "Identifier": "SI-3",
275 "baseline": [{"Low": ["SI-3"]},
276             {"Moderate": ["SI-3", "SI-2"]},
277             {"High": ["SI-3", "SI-2"]}],
278 "question": "Do you protect the information system from malicious code?",
279 "Answer": "Yes",
280 "SecurityTechVendor": "Microsoft",
281 "SecurityTechProduct": "Azure Security center",
282 "SecurityTechVersion": "",
283 "OtherGoal": []
284 }
285 ],
286 "Availability":
287 [{"SecurityControl": "Information system backup",
288 "Identifier": "CP-9",
289 "baseline": [{"Low": ["CP-9"]},
290             {"Moderate": ["CP-9"]},
291             {"High": ["CP-9"]}],
292 "question": "Do you provide any Information system backup?",
293 "Answer": "Yes",
294 "SecurityTechVendor": "ownCloud",
295 "SecurityTechProduct": "ownCloud Server",
296 "SecurityTechVersion": "10.0.1",
297 "OtherGoal": []
298 },
299 {"SecurityControl": "Information system recovery and reconstitution",
300 "Identifier": "CP-10",
301 "baseline": [{"Low": ["CP-10"]},

```

```

302         {"Moderate":["CP-10"]},
303         {"High":["CP-10"]}],
304     "question":"Do you provide any Information system recovery and
reconstitution?",
305 "Answer": "Yes",
306 "SecurityTechVendor": "ownCloud",
307 "SecurityTechProduct": "ownCloud Server",
308 "SecurityTechVersion": "10.0.1",
309 "OtherGoal":[]
310 },
311 { "SecurityControl": "Denial of service protection",
312 "Identifier": "SC-5",
313 "baseline": [{"Low":["SC-5"]},
314             {"Moderate":["SC-5"]},
315             {"High":["SC-5"]}],
316 "question":"Do you secure the communication channel?",
317 "Answer": "Yes",
318 "SecurityTechVendor": "Cisco",
319 "SecurityTechProduct": "firepower management center",
320 "SecurityTechVersion": "6.4.0",
321 "OtherGoal":[]
322 },
323 { // We have put the following control by its family as
324   // the answer to all its memeber were Not applicable.
325   "SecurityControl": "Physical and environmental protection",
326 "Identifier": "PE",
327 "question":"Do you provide any Physical and environmental protection?",
328 "Answer": "Not Applicable",
329 "SecurityTechVendor": "",
330 "SecurityTechProduct": "",
331 "SecurityTechVersion": "",
332 "OtherGoal": ""
333 }],
334 "Likelihood":
335 { "Confidentiality":
336   { "total": "50",
337     "Applicable": "23",
338     "Implemented": "20",
339     "NotImplemented": "3",
340     "LikelihoodLevel": "0.7"
341     "ProtectionLevel": "4.3"

```

```

342 },
343 "Integrity":
344 {
345   "total": "42",
346   "Applicable": "30",
347   "Implemented": "21",
348   "NotImplemented": "9",
349   "LikelihoodLevel": "1.5"
350   "ProtectionLevel": "3.5"
351 },
352 "Availability":
353 {
354   "total": "22",
355   "Applicable": "6",
356   "Implemented": "4",
357   "NotImplemented": "2",
358   "LikelihoodLevel": "1.7"
359   "ProtectionLevel": "3.3"
360   "
361 }
362 }
363 }

```

C.2 Right Questionnaire

Listing C.2: Right Questionnaire responses

```

1 {
2 "Data Unlinkability":
3 [{ "Tactic": "Mix",
4   "question": "Do you Mix personal data to hide the source or their
   interrelationships?",
5   "Answer": "No",
6   "SecurityTechVendor": "",
7   "SecurityTechProduct": "",
8   "SecurityTechVersion": "",
9   "OtherGoal": ""
10 },

```

```

11 { "Tactic": "Dissociate",
12   "question": "Do you Break the link and remove the correlation between
13   events, persons, and data?",
14   "Answer": "Yes",
15   "SecurityTechVendor": "",
16   "SecurityTechProduct": "",
17   "SecurityTechVersion": "",
18   "OtherGoal": ""
19 },
20 { "Tactic": "Obfuscate",
21   "question": "Do you Prevent understandability of personal data?",
22   "Answer": "Not Applicable",
23   "SecurityTechVendor": "",
24   "SecurityTechProduct": "",
25   "SecurityTechVersion": "",
26   "OtherGoal": ""
27 },
28 { "Tactic": "Restrict",
29   "question": "Do you Restrict access to personal data?",
30   "Answer": "Yes",
31   "SecurityTechVendor": "",
32   "SecurityTechProduct": "",
33   "SecurityTechVersion": "",
34   "OtherGoal": ""
35 },
36 { "Tactic": "Isolate",
37   "question": "Do you Collect and process personal data in different
38   databases or applications?",
39   "Answer": "No",
40   "SecurityTechVendor": "",
41   "SecurityTechProduct": "",
42   "SecurityTechVersion": "",
43   "OtherGoal": ""
44 },
45 { "Tactic": "Distribute",
46   "question": "Do you Distribute the collection and processing of personal
47   data over different physical locations?",
48   "Answer": "No",
49   "SecurityTechVendor": "",
50   "SecurityTechProduct": "",
51   "SecurityTechVersion": ""

```

```

49 "OtherGoal": ""
50 },
51 { "Tactic": "Summarise",
52   "question": "Do you Summarise detailed attributes into more coarse-grained
53   , general attributes?",
54   "Answer": "No",
55   "SecurityTechVendor": "",
56   "SecurityTechProduct": "",
57   "SecurityTechVersion": "",
58   "OtherGoal": "Minimization"
59 },
60 { "Tactic": "Group",
61   "question": "Do you Aggregate information about a group of people instead
62   of processing personal information for each person?",
63   "Answer": "Not Applicable",
64   "SecurityTechVendor": "",
65   "SecurityTechProduct": "",
66   "SecurityTechVersion": "",
67   "OtherGoal": "Minimization"
68 },
69 { "Tactic": "Perturb",
70   "question": "Do you process an approximation of personal data or adjust
71   the value with some random noise?",
72   "Answer": "Not Applicable",
73   "SecurityTechVendor": "",
74   "SecurityTechProduct": "",
75   "SecurityTechVersion": "",
76   "OtherGoal": "Minimization"
77 }
78 ],
79 "Minimization":
80 [{ "Tactic": "Select",
81   "question": "Do you Select only relevant people and relevant attributes?",
82   "Answer": "Yes",
83   "SecurityTechVendor": "",
84   "SecurityTechProduct": "",
85   "SecurityTechVersion": "",
86   "OtherGoal": ""
87 },
88 { "Tactic": "Exclude",
89   "question": "Do you Exclude people or attributes that are irrelevant?",

```

```

87  "Answer": "Yes",
88  "SecurityTechVendor": "",
89  "SecurityTechProduct": "",
90  "SecurityTechVersion": "",
91  "OtherGoal": ""
92  },
93  { "Tactic": "Strip",
94    "question": "Do you Determine beforehand the time you need a particular
      personal data item, and automatically delete them as soon as this time
      expires?",
95    "Answer": "Yes",
96    "SecurityTechVendor": "",
97    "SecurityTechProduct": "",
98    "SecurityTechVersion": "",
99    "OtherGoal": "Storage limitation"
100  },
101  { "Tactic": "Destroy",
102    "question": "Do you Remove data as soon as it is no longer necessary?",
103    "Answer": "Yes",
104    "SecurityTechVendor": "",
105    "SecurityTechProduct": "",
106    "SecurityTechVersion": "",
107    "OtherGoal": "Storage limitation"
108  }],
109  "Transparency":
110  [{ "Tactic": "Supply",
111    "question": "Do you Supply information about which personal data is
      processed, how they are processed, and why?",
112    "Answer": "Yes",
113    "SecurityTechVendor": "",
114    "SecurityTechProduct": "",
115    "SecurityTechVersion": "",
116    "OtherGoal": "Purpose Specification"
117  },
118  { "Tactic": "Explain",
119    "question": "Do you argue why processing of these personal data are
      necessary?",
120    "Answer": "Yes",
121    "SecurityTechVendor": "",
122    "SecurityTechProduct": "",
123    "SecurityTechVersion": "",

```

```

124 "OtherGoal": "Purpose Specification"
125 },
126 { "Tactic": "Notify",
127   "question": "Do you Notify users the moment you process their personal
128     data?",
129   "Answer": "No",
130   "SecurityTechVendor": "",
131   "SecurityTechProduct": "",
132   "SecurityTechVersion": "",
133   "OtherGoal": ""
134 },
135 [{"Tactic": "Consent",
136   "question": "Do you Ask users explicit consent to the processing of their
137     personal data?",
138   "Answer": "Yes",
139   "SecurityTechVendor": "",
140   "SecurityTechProduct": "",
141   "SecurityTechVersion": "",
142   "OtherGoal": "Purpose limitation"
143 },
144 { "Tactic": "Choose",
145   "question": "Do you offer user basic functionality to have real choices
146     over their personal data?",
147   "Answer": "No",
148   "SecurityTechVendor": "",
149   "SecurityTechProduct": "",
150   "SecurityTechVersion": "",
151   "OtherGoal": ""
152 },
153 { "Tactic": "Update",
154   "question": "Do you Offer users the means to review and update the
155     personal data?",
156   "Answer": "No",
157   "SecurityTechVendor": "",
158   "SecurityTechProduct": "",
159   "SecurityTechVersion": "",
160   "OtherGoal": ""
161 },
162 { "Tactic": "Retract",

```

```

160     "question": "Do you Offer users a means to retract or to ask for the
        deletion of their personal data?",
161     "Answer": "No",
162     "SecurityTechVendor": "",
163     "SecurityTechProduct": "",
164     "SecurityTechVersion": "",
165     "OtherGoal": ""
166   }],
167   "Accountability":
168   [{ "Tactic": "log",
169     "question": "Do you log all the steps taken?",
170     "Answer": "Yes",
171     "SecurityTechVendor": "",
172     "SecurityTechProduct": "",
173     "SecurityTechVersion": "",
174     "OtherGoal": ""
175   },
176   { "Tactic": "Audit",
177     "question": "Do you Audit the logs regularly?",
178     "Answer": "Yes",
179     "SecurityTechVendor": "",
180     "SecurityTechProduct": "",
181     "SecurityTechVersion": "",
182     "OtherGoal": ""
183   },
184   { "Tactic": "Report",
185     "question": "Do you Report the results of audits to the Data Protection
        Authority?",
186     "Answer": "Yes",
187     "SecurityTechVendor": "",
188     "SecurityTechProduct": "",
189     "SecurityTechVersion": "",
190     "OtherGoal": ""
191   }],
192   "Lawfulness":
193   [{ "Tactic": "Create",
194     "question": "have you created a privacy policy?",
195     "Answer": "Yes",
196     "SecurityTechVendor": "",
197     "SecurityTechProduct": "",
198     "SecurityTechVersion": ""

```

```

199   "OtherGoal": ""
200 },
201 { "Tactic": "Maintain",
202   "question": "Do you Maintain the policy with all the necessary technical
203   and organisational controls?",
204   "Answer": "Yes",
205   "SecurityTechVendor": "",
206   "SecurityTechProduct": "",
207   "SecurityTechVersion": "",
208   "OtherGoal": ""
209 },
210 { "Tactic": "Uphold",
211   "question": "Do you Verify the privacy policy regularly to adjust its
212   implementation whenever necessary?",
213   "Answer": "Yes",
214   "SecurityTechVendor": "",
215   "SecurityTechProduct": "",
216   "SecurityTechVersion": "",
217   "OtherGoal": ""
218 }],
219 "Likelihood":
220 { "Data Unlinkability":
221   {
222     "total": "8",
223     "Applicable": "6",
224     "Implemented": "2",
225     "NotImplemented": "4",
226     "Likelihood": "3.3",
227     "Protection": "1.7"
228   },
229   "Minimization": {
230     "total": "7",
231     "Applicable": "5",
232     "Implemented": "4",
233     "NotImplemented": "1",
234     "Likelihood": "1",
235     "Protection": "4"
236   },
237   "Purpose Specification":
238   {
239     "total": "2",

```

```

238     "Applicable": "2",
239     "Implemented": "2",
240     "NotImplemented": "0",
241     "Likelihood": "0",
242     "Protection": "5"
243 },
244 "Purpose limitation":
245 {
246     "total": "1",
247     "Applicable": "1",
248     "Implemented": "1",
249     "NotImplemented": "0",
250     "Likelihood": "0",
251     "Protection": "5"
252 },
253 "Transparency":
254 {
255     "total": "3",
256     "Applicable": "3",
257     "Implemented": "2",
258     "NotImplemented": "1",
259     "Likelihood": "1.7",
260     "Protection": "3.3"
261 },
262 "Intervenability":
263 {
264     "total": "4",
265     "Applicable": "4",
266     "Implemented": "1",
267     "NotImplemented": "3",
268     "Likelihood": "4",
269     "Protection": "1"
270 },
271 "Lawfulness":
272 {
273     "total": "3",
274     "Applicable": "3",
275     "Implemented": "3",
276     "NotImplemented": "0",
277     "Likelihood": "0",
278     "Protection": "5"

```

```
279 },
280 "Accountability":
281 {
282   "total": "3",
283   "Applicable": "3",
284   "Implemented": "3",
285   "NotImplemented": "0",
286   "Likelihood": "0",
287   "Protection": "5"
288 },
289 "Storage limitation":
290 {
291   "total": "2",
292   "Applicable": "2",
293   "Implemented": "2",
294   "NotImplemented": "0",
295   "Likelihood": "0",
296   "Protection": "5"
297 },
298 }
299 }
```

Appendix D

OAuth/OIDC Related Materials

This chapter gives explains the OAuth/OIDC features and provides the complete OAuth/OIDC reference model.

D.1 OAuth/OIDC Features Description

Table [D.1](#) describe the atomic feature related to OAuth/OIDC standards.

D.2 OAuth/OIDC Complete Reference Model

Table [D.2](#) reports the complete OAuth/OIDC Reference Model which contains response types: code, hybrid, password, client credential and token.

D.3 Complete List of assessed IdMPs

Table [D.3](#) represents a complete list of IdMPs under analysis together with their supported features.

Table D.1: Atomic Features Description.

Atomic Features	Description	Source
code,implicit,client_credentials,password,hybrid	Defined values for the <i>response_type</i> OAuth/OIDC parameter to determine the authorization flow to be used.	[SBJ*14]
state	OAuth/OIDC parameter with an opaque value used to maintain the state between the authorization request and response.	[SBJ*14]
nonce	OIDC parameter with an opaque value used to associate a client session with an <i>id_token</i> .	[SBJ*14]
request	OAuth/OIDC parameter for sending the authorization request parameters in a single parameter and to be optionally signed.	[SBJ*14]
request_uri	OAuth/OIDC parameter to enable authorization requests to be passed by reference. The object value retrieved from the resources at the specified URL.	[SBJ*14]
query	OAuth/OIDC default functionality to serialize the authorization request parameters which add them directly in the request.	[SBJ*14]
form_post,fragment,query	Defined values for the <i>response_mode</i> OAuth parameter to inform the IdMP about the mechanism for returning the parameters from the AS endpoint	[SBJ*14]
plain,S256	Defined values for the <i>code_challenge_method</i> OAuth/OIDC parameter to define the transformation method used to calculate the <i>code_challenge</i> .	[SBA15]
client_secret_jwt,private_key_jwt,mTLS,client_secret_basic,client_secret_post	A set of client authentication methods that are introduced by OAuth/OIDC to authenticate the clients at the Token endpoint.	[SBJ*14,CBSL19]
code_verifier	OAuth/OIDC parameter that contains a high-entropy cryptographically created string that is unique for each authorization request.	[SBA15]
fullredirect_uri,pattern redirect_uri	Defines the redirection URL registration policy within the IdMP developer console.	[LBLEF21]
binding IdMP metadata	App developers must bind IdMP metadata for each authorization request which are sent to AS by setting them in <i>UA</i> header.	[LBLEF21]
referrer	App developers must set the <i>Referrer-Policy</i> HTTP header into <i>no-referrer</i> .	[LBLEF21]
distinct redirect_uri	App developers must register distinct <i>redirect_uri</i> per each IdMP.	[LBLEF21]
open redirect validation	App developers must avoid the acceptance of arbitrary value by the registered <i>redirect_uri</i> of the client and creates a redirect to it.	[LBLEF21]
state validation	App developers must validate the equality of the <i>state</i> parameter value in the authorization request and response.	[Har12]
storing IdMP metadata	App developers must store the IdMP metadata that they send the request and check if the request was received from the correct IdMP.	[LBLEF21]
issuer validation	App developers must verify the equality of the returned issuer value with the IdMP that they communicate.	[LBLEF21]
id token validation	App developers must verify all the claims within the <i>id_token</i> by following the 13 recommendations within OIDC document.	[SBJ*14]
claims	OIDC parameter to enable requesting individual claims to be returned from the User info and/or in <i>id_token</i> .	[SBJ*14]
scope	OAuth/OIDC parameter that contains string values to specify the scope of the <i>access_token</i> .	[SBJ*14]
purpose	OIDC parameter to enable stating the purpose of asking the specific claim by the client.	[LF20]
verified_claims	OIDC parameter that contains object or array of one or more verified claims.	[LF20]
vot,acr	OAuth/OIDC parameters to request IdMP for guaranteeing a certain level of identity proofing.	[SBJ*14,RJ18]
login,select_account,consent	Defined values for the <i>prompt</i> OAuth/OIDC parameter to specify whether IdMPs prompt end-users for re-authentication and consent.	[SBJ*14]
pairwise,public	Defined values for the <i>subject_type</i> OIDC parameter to determine how the application unique identifier is generated by the IdP.	[SBJ*14]

D.4 IdMP_Doc Questionnaire

Following listing represent the *IdMP_Doc Questionnaire*.

Table D.2: OAuth/OIDC Full Reference Model.

Deployment Place	Atomic Features	Threat (T)	Goal (G)	Consecutive T	Consecutive G	PL	LL
Security Feature							
Authorization Request	code	Obtain AT	PD Conf	-	-	3	3
	token					1	
	client_credentials					3	
	password					1	
	hybrid	Obtain AT , Session misuse	PD Conf	-	-	3	5
	nonce					5	
	state	Session misuse	PD Conf	-	-	5	5
	request ^{c,hyd}					5	
	request_uri ^{c,hyd}	Obtain code	AT Conf	Obtain AT	PD Conf	5	5
	query ^{c,hyd}					1	
	request ^{i,pswd}	Obtain AT	PD Conf	-	-	3	5
	request_uri ^{i,pswd}					3	
	query ^{i,pswd}	Obtain Code	AT Conf	Obtain AT	PD Conf	1	5
	form_post ^{c,hyd}					5	
	fragment ^{c,hyd}					1	
	query ^{c,hyd}					1	
Token Request	form_post ⁱ	Obtain AT	PD Conf	-	-	5	5
	fragment ⁱ					1	
	Plain	Obtain AT , Session misuse	PD Conf	-	-	1	5
	S256					5	
	mTLS	Obtain AT	PD Conf	-	-	3	3
	client_secret_jwt					3	
	private_key_jwt					3	
	client_secret_basic					2	
	client_secret_post	Obtain AT , Session misuse	PD Conf	-	-	2	5
	code_verifier					5	
Authorization Request/ Token Request	full_redirect_uri ^{idmp,c,hyd}	Obtain Code	AT Conf	Obtain AT	PD Conf	3	3
	pattern_redirect_uri ^{idmp,c,hyd}					1	
	full_redirect_uri ^{idmp,i}	Obtain AT	PD Conf	-	-	2	2
	pattern_redirect_uri ^{idmp,i}					1	
Header	binding IdMP metadata ^{cl,c,hyd}	Obtain Code	AT Conf	Obtain AT	PD Conf	2	2
	binding IdMP metadata ^{cl,i}	Obtain AT	PD Conf	-	-	2	2
	referrer ^{cl,c,hyd}	Obtain Code	AT Conf	Obtain AT	PD Conf	3	3
Console	referrer ^{cl,i}	Obtain AT	PD Conf	-	-	2	2
	distinct_redirect_uri ^{cl,c,hyd}	Obtain Code	AT Conf	Obtain AT	PD Conf	5	5
	distinct_redirect_uri ^{cl,i}	Obtain AT	PD Conf	-	-	2	2
Client Check	open_redirect_validation ^{cl,c,hyd}	Obtain Code	AT Conf	Obtain AT	PD Conf	5	5
	open_redirect_validation ^{cl,i}	Obtain AT	PD Conf	-	-	2	2
	state Validation ^{cl,c,hyd}	Obtain Code	PD Conf	-	-	5	5
	state validation ^{cl,i}	Obtain AT	PD Conf	-	-	5	5
	storing IdMP metadata ^{cl,c,hyd}	Obtain Code	AT Conf	Obtain AT	PD Conf	5	5
	storing IdMP metadata ^{cl,i}	Obtain AT	PD Conf	-	-	5	5
	issuer validation ^{cl}	Obtain Code	AT Conf	Obtain AT	PD Conf	5	5
	id token validation ^{cl}	Impersonation	PD Conf	-	-	5	5
Privacy Feature							
Authorization Request	claims	Comp data mini	Data mini	-	-	5	5
	scope	Comp data mini	Data mini	-	-	5	5
	purpose	Comp Pur spec, Trans	Pur spec, Trans	-	-	5	5
	verified_claims	Comp PD accu	PD accu	-	-	5	5
	vot	Impersonation, Comp PD accu	PD accu, PD Conf	-	-	5	5
	acr					5	
	login	Comp Transparency	Transparency	-	-	3	3
console	select_account					3	
	consent	Linkability	Unlinkability	-	-	5	5
	pairwise					1	
	public	Linkability	Unlinkability	-	-	5	5
	public					1	

LEGEND. idmp: idmp only feature, cl: client only feature, c: code, i: implicit, hyd: hybrid, pswd: password comp: compromise, PD: personal data, AT: access token, trans: transparency, data mini: data minimization, conf: confidentiality, pur spec: purpose specification, PL: protection level, LL: likelihood level

Listing D.1: IdMP_Doc Questionnaire.

1. Does the IdP support code Flow?	1
2. Does the IdP support implicit Flow?	2
3. Does the IdP support client credential Flow?	3
4. Does the IdP support password Flow?	4
5. Does the IdP support hybrid Flow?	5
6. Does the IdP support mTLS client authentication method?	6
7. Does the IdP support client_secret_jwt client authentication method?	7
8. Does the IdP support private_key_jwt client authentication method?	8
9. Does the IdP support client_secret_basic client authentication method?	9
10. Does the IdP support client_secret_post client authentication method?	10
11. Does the IdP support SHAS256 for code challenge method?	11
12. Does the IdP support plain for code challenge method?	12
13. Does the IdP support request parameter?	13
14. Does the IdP support request_uri parameter?	14
15. Does the IdP support query parameter?	15
16. Does the IdP support subject_type=pairwise?	16
17. Does the IdP support subject_type=public?	17
18. Does the IdP support verified_claims parameter?	18
19. Does the IdP support purpose parameter?	19
20. Does the IdP support acr parameter?	20
21. Does the IdP support vot parameter?	21
22. Does the IdP support claims parameter?	22
23. Does the IdP support scope parameter?	23

D.5 IdMP_ToAsk Questionnaire

Listing [D.2](#) represents the questions.

Listing D.2: The IdMP_ToAsk_Questionnaire.

1. Does the IdMP support full redirect_uri?	1
2. Does the IdMP support pattern redirect_uri?	2
3. Does the IdMP support nonce parameter?	3
4. Does the IdMP support state parameter?	4
5. Does the IdMP support query response mode?	5
6. Does the IdMP support form_post response mode?	6
7. Does the IdMP support fragment response mode?	7

8. Does the IdMP support login for prompt parameter?	8
9. Does the IdMP support select_account for prompt parameter?	9
10. Does the IdMP support consent for prompt parameter?	10

Table D.3: list of known IdMPs and their supported features.

Atomic Feature	Authlete	Forge	Rock	Cloudidentity	Connect2id	WSO2	PING	IBM	Google	Facebook	Yahoo	Amazon	LinkedIn	Microsoft	DropBox	OKTA	Auth0	Box	Hidrive	BeeMinder
code	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T*	F
implicit	T	T	T	T	T	T	T	T	T	T*	T	T	T	T	T	T	T	T	F	T
client_credential	T	T	T	T	T	T	T	T	T	F	F	F	F	F	F	F	F	F	F	F
password	T	T	T	T	T	T	T	T	T	F	F	F	F	F	F	F	F	F	F	F
hybrid	T	T	T	T	T	T	T	T	T	F	F	F	F	F	F	F	F	F	F	F
mtls	T	T	T	T	T	T	T	T	T	F	F	F	F	F	F	F	F	F	F	NA
client_secret_basic	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	NA
client_secret_post	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	NA
client_secret_jwt	T	F	T	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	NA
private_key_jwt	T	T	T	T	T	T	T	T	T	F	F	F	F	F	F	F	F	F	F	NA
plain	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	NA
S256	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	NA
request	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	F
request_uri	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	F
query	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	F
claim	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	F
scope	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	F
purpose	T	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
verified_claims	T	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
acr	T	T	T	T	T	T	T	T	T	F	F	F	F	F	F	F	F	F	F	F
vot	F	F	T	F	T	T	T	T	T	F	F	F	F	F	F	T	T	F	F	F
public	T	T	T	T	T	T	T	T	T	NA	T	T	NA	F	NA	T	T	NA	NA	NA
pairwise	T	T	T	T	T	T	T	T	T	NA	F	F	NA	T	NA	F	F	NA	NA	NA
<i>Sensitive Sector</i>	<i>Yes</i>	<i>Yes</i>	<i>Yes</i>	<i>Yes</i>	<i>Yes</i>	<i>Yes</i>	<i>Yes</i>	<i>Yes</i>	<i>No</i>	<i>No</i>	<i>No</i>	<i>No</i>	<i>No</i>	<i>No</i>	<i>No</i>	<i>Yes</i>	<i>Yes</i>	<i>No</i>	<i>No</i>	<i>No</i>

LEGEND. T: opt-supported but not enforced, T*:not follow the standard definition, NA: not applicable