TECHNICAL UNIVERSITY - VARNA

AUTHOR:
Kadir Ider

TITLE:

Complexity Reduction and Operationalization of the GDPR: Conceptualization of a User-Oriented Online Privacy Control System and Evaluation of its Effects on Corporate Trust

ABSTRACT of a dissertation for obtaining educational and PhD degree

Doctoral Programme 05.02.21
"Organization and Management of Production (Industry)"
in professional field 5.13 "General Engineering"

Scientific supervisors:
Prof. Todor Ganchev, PhD;
Prof. Svetlana Lesidrenska, PhD

Reviewers:
1. **Prof. Siyka Demirova, PhD**
2. **Assoc. Prof. Kapka Manasieva, PhD**

Varna, 15.02.2023

The dissertation defense will take place on ..... at ....
in an open meeting of a jury formed by order of the Rector No. ...../.....
The defense materials (the dissertation, reviews and opinions) are available to those interested at the Doctoral Center, Room 318 NUC

Table of Content

A. CHARACTERISTIC OF THE THESIS

This dissertation aims to develop a user-centric privacy control system that helps organizations comply with GDPR. The study uses literature review, primary and secondary data collection and analysis, and design thinking to create a practical, scalable, and cross-industry-applicable privacy control system that considers the societal impact of privacy, fuzzy regulations, and technology. The research methodology includes an international web-based survey using Qualtrics and Google Forms to understand user privacy awareness, trust towards organizations, and evaluation of privacy control elements.

The dissertation consists of four chapters. Chapter 1 provides a general overview of the dissertation's purpose and background. Chapter 2 defines relevant terms used in the research, such as "user," "organization," "control," "trust," "trustworthiness," and "measurement framework." Chapter 3 outlines the methodology used for collecting and analyzing data on users' and organizations' trustworthiness-building factors. Chapter 4 summarizes the study results, proposes a future development plan, and concludes by highlighting the need for a task force to research user needs and organizational challenges.

The dissertation brings a novel and practical approach to the challenges in GDPR compliance by integrating societal impact of privacy, decreasing the burden of fuzzy regulations, and technology into a user-centric system. The proposed privacy control system will empower individuals to control their personal data, countering the trend of control shifting to data processing organizations. The study's results provide insights into users' privacy awareness and behavior, and their trust towards organizations, which will inform the development of the user-centric privacy control system.

In conclusion, this dissertation contributes to the GDPR compliance discussion by proposing a practical and user-centric approach to privacy control systems. The study provides insights into users' privacy awareness and behavior, and their trust towards organizations, which can be used to enhance individual control over personal data and promote trust between individuals and organizations.

The problems addressed in the dissertation research therefore can be concluded as follows:

1. The societal impact of privacy, uncovering the lack of user-centricity and focus on increasing numbers of data collection endpoints,
2. Fuzzy regulations and lack of practical guidance, reflecting the challenge to understand and translate requirements into operational processes, lawfully and consistently,
3. Technology as the enabler and obstacle, highlighting lagging information system infrastructures at the core of an effective protection mechanism.

B. OBJECT AND SUBJECT OF STUDY

The object of this study is the development of a user-centric privacy control system to assist organizations in complying with the General Data Protection Regulation (GDPR). The subject of the research is the practical, scalable, and cross-industry-applicable privacy control system, which considers the societal impact of privacy, fuzzy regulations, and technology. To achieve this objective, the study incorporated a literature review, primary and secondary data collection and analysis, and design thinking.

The study's focus on making GDPR compliance practical and scalable is significant, as it is essential for organizations to maintain user privacy while adhering to regulations. Furthermore, the study's emphasis on a user-centric privacy control system that takes into account user privacy awareness, trust towards organizations, and privacy control elements is an innovative and practical approach to GDPR compliance challenges. The study also provides valuable insights into users' privacy awareness and behavior, which will aid in the development of the privacy control system.

The main theoretical and methodological issues concerning the privacy control system concept are as following**:**

- The research will be conducted through a series of international surveys, a systematic literature review, and a design thinking process. The resulting framework will be evaluated through a prototype implementation.
- Definitions are drawn from the GDPR regulation, the Article 29 Working Party, and social learning theory.
- Assessment of external research results and comprehensive market studies
- Analysis of legal and technical control elements
- Evaluation of psychological control through surveys and studies

While the study itself is planned and executed from within the European Union (EU), the method of analysis considers views of non-EU residents and their understanding of a privacy control system as well as its effects on corporate trustworthiness. This approach ensures a wider applicability, thus, expanding the territorial usage potentials.

C. PUBLICATIONS ON THE THESIS

1) Ider, K. (2022). Assessment of the quality of user awareness of GDPR in healthcare IOT. In Proceedings of the International Conference on Biomedical Innovations and Applications (BIA-2021) (pp. 1-6). IEEE. https://doi.org/10.1109/BIA52594.2022.9831287

2) Ider, K. (2021). Secure Public WiFi durch Network Access Control – Ansätze, Chancen und datenschutz-rechtliche Implikationen. In Proceedings of the Nachwuchswissenschaftler*innenkonferenz 2020/21, EAH Jena.

3) Ider, K., & Faustino-Bauer, M. (2020). DSGVO Compliance und Datenschutz-Managementsystem als Erfolgsfaktor für die Digitale Transformation nutzen. ZRFC Risk, Fraud & Compliance Magazine, 75(6), 327-332. https://doi.org/10.37307/j.1867-8394.2020.06.04

4) Ider, K., & Schmietendorf, A. (2020). Data Privacy For AI Fraud Detection Models – A framework for GDPR compliant AI. In Proceedings of the Fourteenth International Conference on Digital Society (ICDS 2020) (pp. 17-22). IARIA XPS Press. ISBN: 978-1-61208-760-3

5) Ider, K. (2020). Effective Privacy Management Concepts: Increasing Privacy Control by Reducing Complexity. In Proceedings of the 2020 Evaluation of Service-APIs (ESAPI) of the Central Europe Computer Measurement Group (ceCMG) (pp. 143-148). Shaker Verlag GmbH. ISBN: 978-3-8440-7515-1

6) Ider, K. (2019). Barriers for the Utilization of Open Data. In Proceedings of the 2019 Evaluation of Service-APIs (ESAPI) of the Central Europe Computer Measurement Group (ceCMG) in cooperation with Hochschule für Technik und Wirtschaft Dresden (pp. 97-102). Shaker Verlag GmbH. ISBN: 978-3-8440-6837-5

D. GENERAL CHARACTERISTICS OF THE DISSERTATION

I. Approval of the Development

The dissertation work was reported and discussed in its separate parts and in its completed form at a meeting of the Departmental Council of the Department of Industrial Management at the Faculty of Mechanical Engineering and Technology of the Technical University of Varna.

II. Brief Outline of the Thesis

The structure of the thesis comprises a sequence of chapters that conform to a prescribed set of rules, which are:

1) Emphasizes the scope, methods, results, and novelty of each chapter in the research
2) Includes a conclusion for each chapter that summarizes the advances and results
3) Summarizes the advances resulting from the PhD research

1. Chapter: Introduction To Dissertation

With the introduction of a standardized General Data Protection Regulation (GDPR), the European Parliament seeks to enforce stricter accountability compliance in the processing of personal information. Consequently, organizations need to ensure adequate and effective communication of privacy terms to build an appropriate level of trust in individuals. The territorial scope of the regulation extends to foreign companies, which offer goods and services to EU residents. A subsequent non-compliance can result in fines, of which a cumulative 1.6 billion Euros have been paid as of mid 2022 (Ider, 2020b).

The introduction of a Europe-wide standardized data protection regulation is a meaningful step as the rising number of personal devices and progressive digitization of services add additional verticals for personal data collection and thus, such data needs to be protected. As of 2020, 90% of all European residents regularly access the internet, primarily via mobile phone, followed by desktop PC and marginally by tablet (ContentSquare, 2020; Kemp, 2020). In Germany, where every person has access to more than seven (internet-connected) devices, households consist of two members on average. While some devices are used mutually, approximately two personal mobile phones are attributable solely to each person (Werliin & Kokholm, 2020, p.10; Statistisches Bundesamt (Destatis), 2020, p.44). The three most common digital services accessed are entertainment, product purchases and banking transactions (Betti et al., 2020).

Due to the growing data access points, data collection and processing methodologies, the regulation aims at improving data protection. However, nearly 2.5 years after introducing

the GDPR, ⅔ of all German organizations still struggle to meet full compliance (Dehmel & Kelber, 2020, p2). The conclusion can be drawn that a similar level of compliance is existent across European organizations, considering the increasing number of imposed fines Europe-wide (Ider, 2020a, p.105).

Therefore, this dissertation is dedicated to provide a framework to reduce the complexity and improve operationalization of the European Data Protection Regulation (GDPR). This is achieved through the conceptual development of a pragmatic, scalable and cross-industry-applicable user-centric privacy control system with minimally disruptive organizational design properties. The topic and the underlying research have a contemporary significance and immediate societal impact. Currently, both users and organizations are affected by three aspects, which further substantiate the main drivers for research. These include the fuzzy regulations and lack of practical guidance, technological challenges, and the data protection compliance dilemma.

2. Analytical Research And Review Of The Global And Regional Solutions To The Problem

2.1. Problem Statement

The GDPR is not designed to provide practical guidance for the implementation of compliant systems and procedures. It instead lays down the principles for data processing, i.e., focusing on “what criteria must be fulfilled” but lacks “how it should be done”.

There is no global or industry-wide end-to-end implementation consensus regarding the communication of privacy modalities at the current research time. Affected organizations, therefore, struggle with the interpretation of the regulation and associated legal obligations and consequently with the adaptation of existing IT infrastructures (Jiang et al., 2019, p13). Almost 40% of the 1100 interviewed organizations claim that one of the most significant difficulties is reconciling the existing IT infrastructure with the GDPR (Jiang et al., 2019, p.13).

The lack of legal and technical understanding of the GDPR causes a misalignment of compliance system design and operative effectiveness. Despite the efforts of organizations to compliantly communicate privacy matters to individuals, the current juridical uncertainty leads to excessive legal language in the policies as such documents are often written by such professionals (Faustino-Bauer & Ider, 2020, p.248). This condition brings about the reverse effect, i.e., non-compliance, due to being unintelligible and complex, thus creates ineffective policies. Organizations, therefore, adversely violate the principles of data processing according to Art. 5 GDPR. Concluding the current challenges, the major cornerstones of the data protection compliance dilemma are:

1) the societal impact of privacy, uncovering the lack of user-centricity and focus on increasing numbers of data collection endpoints,
2) fuzzy regulations and lack of practical guidance, reflecting the challenge to understand and translate requirements into operational processes, lawfully and consistently,
3) technology as the enabler and obstacle, highlighting lagging information system infrastructures at the core of an effective protection mechanism.

2.2. State of Research

Organizations look for possibilities to achieve a competitive advantage by generating valuable insights on individuals as data is recognized as "the new oil" of the 21st century. Building proper tools to compliantly utilize the data is the motivation of this research. At its core, it is about addressing the needs of society and contributing to the better protection of GDPR rights. It aims to establish a fair framework for personal data processing that will improve the current GDPR procedures and their communication for the benefit of the average citizen, public organizations, and all business entities. The current research aims at providing the much-needed application oriented social innovation for the improvement of data protection and better privacy.

The research work in user-centric data management solutions can be grouped into three main areas (Ider, 2020a, p.104). First, models based on Mechanisms for Personal Data Storage (MPDS), second, User-Centric Secure Data Sharing (UCSDS) (Grashöfer et al., 2017, p.1244) and third, Cryptographically Based Solutions (CBS) for creating data transparency and traceability (Truong et al., 2020, p.1746).

The first concept, MPDS, includes solutions, such as Solid (Sambra et al., 2016), Digi.me or Mecco (Sjöberg et al., 2017), which essentially provide socially linked and personal micro-databases for individuals to store and disclose selected data to service providers from a centrally accessible interface. Secondly, UCSDS puts the focus on the infrastructure for data access and an authorization mechanism, thus, stressing less on actual data ownership and more on a technological solution for simplifying the sharing of individual personal data points or categories. The third option, i.e., the CBS, aims at always keeping data usage traceable. The presented solutions, including MPDS, CBS, UCSDS are plotted on the user-controllability and technological-requirements dimensions as displayed in Figure 1. The plot shows the level of user control over their data relative to the amount of expected disruption of an organization's IT infrastructure for achieving user privacy control.

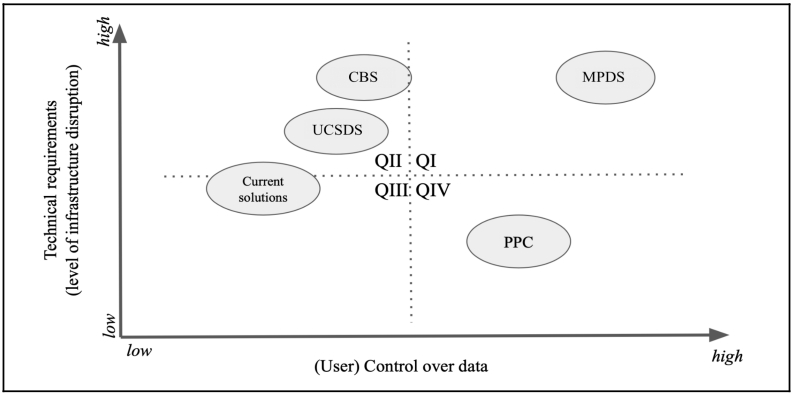

Figure 1: Adaptation Probability of Privacy System

2.3. Benchmarking of Models

A cross-industry-based assessment of contemporary privacy compliance-readiness of German organizations, labeled as "Current solutions", is plotted in Figure 1 for benchmarking purposes. The readiness itself results from the ability to guarantee following GDPR requirements either fully, partially, or not at all (PricewaterhouseCoopers, 2018):

1. Technical and Organizational Security (TOMs),
2. Records of Processing Activities (RoPAs),
3. deletion and retention systems,
4. user rights for data access.

The generated comprehension provides insights for determining the level of "control over data" as well as the underlying "technical requirements", as displayed in the bubble in Figure 1, "Current solutions". The Personal Privacy Cockpit (PPC) is plotted additionally. It is placed near the center of QIV, as it represents the envisaged level of control and technical complexity to be achieved. Figure 1 subdivides the two-dimensional graph into four quadrants. It highlights that the presented solutions within QI and QII inherently require higher technology adaptation, thus, potentially disrupting existing infrastructures to a greater extent. Although MPDS offers the most significant privacy control, it can be concluded that it is not necessarily the most desired solution, because of its inherent technical complexity. Many organizations already see the greatest challenge in the IT infrastructure adaptation. Currently, most organizations can be classified in the QIII segment and should aim to move further towards QIV, through the limitation of technical convolutions and increasing user

access as well as controllability over their data. All options provide important building blocks for developing an effective, trust-forming, secure, transparent, and user-centric solution (Ider, 2020a, p.104). However, these alternatives are subject to more stringent technological requirements, lacking capabilities for mass-adaptation of organizations and users. In addition, the identified solutions are not primarily designed for achieving GDPR compliance.

The conclusion drawn from the foregoing assessment is that significantly greater adoption rates can be achieved if a data protection-friendly solution increases user control proportionally more than the increase in technical complexity. Latter shall further cause fewer disruption through reduction of complex technology requirements. Existing privacy control concepts and services provide important elements, which will be considered in the scope of this research. Nevertheless, this conceptualization aims at reducing technological complexity for both organizations and individuals.

2.4. Research Limitations

The research is limited to a theoretical conceptualization of a user-centric online privacy control system. Consequently, the development and testing of the solution will take place with a smaller sample size. Multiple surveys will be conducted throughout the research to reflect and build in user-specific requirements, ensuring state-of-the-art technology integration. Moreover, the ability to successfully implement the privacy control system into organizations will occur through a theoretical assessment of the features of information technology (IT) system infrastructure and subsequent evaluation of the compatibility between the privacy system and IT. In this context, the underlying premise is that the organizations can demonstrate a minimum level of technical expertise.

The limited time and access to statistical data as well as the resource constraints may affect the representativeness of the research. Cultural preferences or biases may influence the objectivity of the results. Lastly, the gathered data consists of feedback provided by survey participants and thus the evaluation will primarily be conducted based on self-reported rather than observed behavior. To counter measure this possible attitude versus behavior dichotomy (Kokolakis, 2017, p. 124), some questions will be designed in such a way that requires the survey participants to actively engage with the user interface. Consequently, the residual risk is that the obtained data may not entirely reflect actual behavior as the questions are for the purpose of research rather than an actual event where individuals are asked to share data for (e.g., signing up at a website to receive services).

Consequently, self-reported behavior for the purpose of research may be different from that of an observed one. To minimize the dichotomy, the survey aims at simulating “real-life” circumstances to encourage actual user behavior. Thus, survey questions are partially designed to capture self-reported opinions (attitudes) from a user perspective and to some extent detect behavioral insights through active engagement with survey questions, resp.

Incorporated mock ups of system interfaces. The survey design aims to further minimize any work-related association, thus, participants will be offered to freely provide their email addresses, if they plan to participate in the raffle in the scope of the research[1]. The proportional number of users that will enter their data will further provide evidence and validation for the whole data set.

2.5. Chapter Summary

- Scope:
  - Discusses the importance of privacy in the digital age, highlighting the growing need for individuals to approve data collection.
  - Discusses the challenges organizations face in complying with the General Data Protection Regulation (GDPR) and the limited understanding of privacy policies by individuals.
- Methods:
  - Primary and secondary data collection and analysis, systematic literature review, and design thinking process.
- Results:
  - Scope definition, i.e., the dissertation will result in a conceptualization of a pragmatic, scalable, and cross-industry-applicable privacy control system that improves the communication of privacy terms and reduces the complexity of the GDPR.
- Novelty:
  - The study brings a novel and practical approach to the current challenges in GDPR compliance by integrating the societal impact of privacy, decreasing the burden of fuzzy regulations, and technology into a user-centric privacy control system.
- Conclusion:
  - This chapter highlights the importance of privacy and the challenges organizations face in complying with the GDPR. The research aims to address these challenges by developing a user-centric privacy control system.

[1] Survey participants can win online shopping vouchers.

3. Chapter: Theoretical Formulation Of The Decision And Tasks To Achieve The Goal

The following chapter identifies relevant terms and provides their definitions. Based on the findings, the data protection requirements, and the impact of the GDPR on the user privacy system are also determined.

3.1. Terminology Definitions

3.1.1. Definitions of "User"

In the scope of this research the term "user" always refers to a "natural person" and is equivalently used for respondent, survey participant and "data subject".
The term natural person is inferable from Art. 4 (1) GDPR. It stands for any individual that discloses any personal information to an organization in exchange for both paid or free of charge products or services. In the context of Art. 4 (1) GDPR, a natural person or data subject exists, where one or more information leads to unambiguous identification of that individual. The original definition of the regulation is as follows:

> […] 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Consequently, the privacy control system should flag or label special categories of data and provide detailed information on the underlying processing and the enhanced security measures for the protection of such data. The Article 29 Working Party provides a comprehensive definition for indirect user identification, which include (Papers of the Article 29 Working Party, 2014, p.18):

- Single-out: Is it still possible to single out an individual?
- Link: Is it still possible to link records relating to an individual?
- Infer: Can information be inferred concerning an individual?

3.1.2. Definition of Organization

The term "organization" in the scope of this research refers to any institution that processes personal data and does refer as well to all controller types, processors, and their obligations. In the context of the GDPR, the construct of controller and processor is essentially designed to define the obligations and responsibilities among organizations that are

involved in the processing of personal information. The GDPR defines in Art. 4 (7) that a controller is an institution that determines the purpose and means of the processing.

The processor does not determine any of the factors but is a service contractor operating on behalf of the controller.

3.1.3. Definition of Control

In the subchapters of the dissertation the term control is defined from a legal, a technical and a psychological angle. Understanding such definitions is essential to formulating relevant key segments for the assessment of organizational trustworthiness. A summary of key points is provided below:

A. Legal Definition of User Control
   - user rights are specified in Art. 12 – 23 GDPR
   - build the basis for the definition of the user control requirements

B. Psychological Definition of User Control
   - encompasses emotional assessment, which is considered a psychological state
     - authority, power, or influence over events, behaviors, situations, or people
     - regulation [...] of [an] independent variable [...]

C. Technological Definition of User Control
   - physical means to meet the control requirements identified in the legal context
   - refers to the features that an information processing system provides to
     - manage data and maintain underlying systems and
     - allow ownership and transparency of data in the user context
   - ensuring control on an organizational, operational (business process) and information system level.

The three points of view are selected based on the preceding analysis results. The control assessment from the legal perspective is important as it lays down the juridical foundation from which technical and user control elements are derived. Discussed in the dissertation in detail, it is revealed that technical control is the enabler and determines the degree of data management by users or organizations. The psychological perspective determines the awareness and perception of control, which could be considered as the most sensitive aspect. The findings will lead to the evaluation of whether the level of control individuals have over their personal data, corporate processes and systems has an impact on organizations' trustworthiness.

3.1.4. Definition of Trust, Trustworthiness, and the Measurement Framework

In social learning theory trust[2] is formed by the expectation of an outcome of a situation as well as the amount of experience in similar cross-situational circumstances (Rotter, 1980, p.2). A crucial element to forming trust is the confidence in the truthfulness of trust (Rotter, 1980, p.4) in a person or institution, i.e., to what extent someone is trustworthy. Consequently, it can be expected that (1) a trustee's experience, (2) the result that one expects and (3) the level of the trustor's trustworthiness determines the degree of trust.

Due to that, trust particularly differs among different age groups (Sutter & Kocher, 2007, p.373) or occupations of individuals, as it can be expected that age and experience are positively correlated (Gul, 1983, p.86). Experience is assumed to be reflected by a combination of an individual's age and occupation associated with objectives of this research.

In more recent definitions, trust is seen as a social preference (Ashraf et al., 2006, p.194) that replaces the expectation of a return with the altruistic behavior of individuals, placing in the frontline intrinsic selflessness and joy to be good and fair to others (Andreoni & Miller, 2002, p.737). However, the more recent definitions are less suitable for this research, because the object of research is not to investigate the altruistic capacity of individuals towards organizations, but to ascertain a precise terminological definition and further scope the range of applicability of this research.

3.2. Conclusion of Paragraph

Based on the key elements identified in the introductory chapter, the definitions of terms and concepts provided a comprehensive understanding of trust and control from a variety of disciplines, including psychology and technology as well as an interdisciplinary legal perspective.

The definitions were implemented into a multidimensional framework, which will be used as the working model for the subsequent analysis. The technical and psychological insights have further been mapped to the GDPR requirements. An integration of these dimensions ensures a holistic analysis approach and further specification of precise measures and features for the privacy control system. The colors represent the level of influence a party has on the development of trustworthiness. The parties include users, organizations and juridical bodies that define the legislative basis for the GDPR. Moreover, the interim conclusion in the scope of the dissertation reveals that the subsequent assessment can be narrowed down to further in-depth analysis based on (1) age group, (2) occupation and (3) device usership (z-axis).

[2] To ensure a focused and delineated scope of application, this definition does not consider the field dependence (e.g., Gul, 1983), i.e., the extent to which cross-situational circumstances are affected by external influences rather than a personal sense of order.

Therefore, the following paragraphs will provide a three-staged assessment, where the data exploration will take place based on the three segments.

The conclusion will summarize each finding and a subsequent comparison and discussion. The existing framework is therefore extended by the addition of a third dimension, or z-axis. This dimension stipulates the three criteria upon which the trustworthiness-creating elements (represented by the x- and y-axis) are evaluated, as summarized in figure 2.

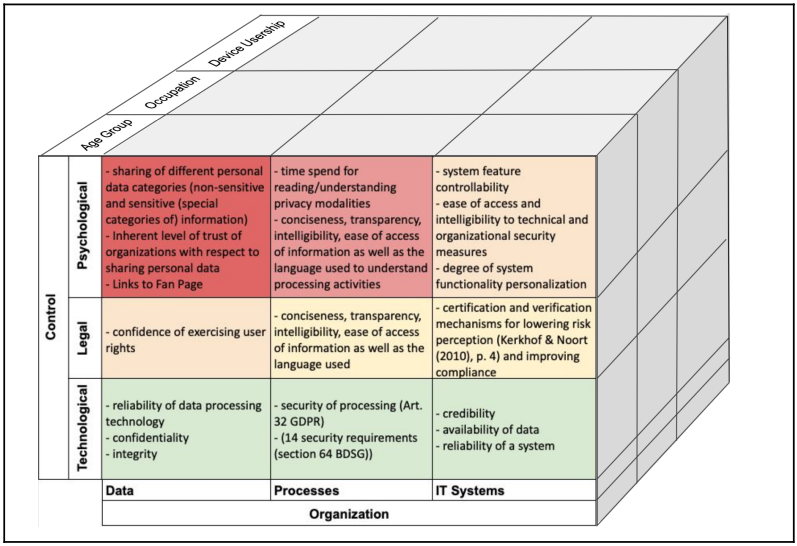

Figure 1: A 3D Concept of Trustworthiness Building Factors

3.3. Chapter Summary

- Scope:
  - This chapter focuses on defining relevant terms in the research such as "user," "organization," "control," "trust," "trustworthiness," and "measurement framework".
  - It further deals with the impact of GDPR on the privacy system and the data protection requirements.
- Methods:
  - Definitions drawn from GDPR regulation, Article 29 Working Party, and social learning theory.
- Results:
  - Three perspectives (legal, psychological, and technological) are used to

evaluate the impact of users' control over personal data and its effects on organizational trustworthiness.

- Novelty:
    - Highlights the importance of considering the three perspectives in evaluating organizational trustworthiness and reveals impact on trustworthiness of control over personal data, processes, and systems.

4. Chapter: Conditions And Environment For Implementing The Solution

In order to tackle the issues highlighted in the introduction, dedicated surveys are designed to collect necessary data to understand the needs from a user perspective as well define a framework and determine working packages for organizations. Therefore, the focus of this chapter will be placed on the methodology of the data collection process, survey design and data analysis structure.

The high-level methodology includes an examination of data and its structure via a descriptive and analytical approach. Qualtrics Stats iQ is mainly used, which features the visualization of numbers, ranks and categories as well as allows cross-tab analysis.

The study begins with outlining the methods used for data collection, followed by a descriptive assessment of the obtained data. The first section discusses data collection instruments and procedures, while the second section presents data using various techniques to draw conclusions and identify patterns.

The third section explores the relationship between the responses. Many possible relationships are explored, whereas statistically significant or otherwise meaningful insights are presented, including visualization.

The fourth section derives insights for the concretization of trustworthiness-building factors, through the preceding response analysis, determination of the weights and identification of their impact on the control system. In the course of this report, it will be further demonstrated how the data analysis results are used to construct a workable framework (see figure 5).

4.1. Introduction to Research Methodology

In March and April 2021 an international web-based survey was conducted and distributed via Qualtrics and Google Forms. Both surveys are identically structured, to ensure that the collected data quality and quantity is comparable. The survey consists of 25 questions with 84 subcategories, clustered into four sections, including the introduction page. The Qualtrics survey link is solely shared among users working in an internal technology organization, operating with various brands in more than 50 countries. The Google Forms link is shared with a wider public group and made available mainly on LinkedIn and Twitter, as

well as various other social platforms by commenting on relevant posts. The demographic questions on the first page are obligatory, subsequent questions can be skipped or answered partially.

The three privacy sections are designed to generate insights for the concretization of trustworthiness-building factors, discussed in the preceding chapters. Each section has its particular focus area and incorporates validation questions to determine users' answers. Each trustworthiness-building factor, i.e., the control and the data processing organization as well as their respective dimensions, i.e., x-axis (data, processes, and IT systems) and y-axis (psychological, legal, technological), exhibits an intersection with the individuals. Consequently, the user's understanding of each dimension, their perception and actual level of control over the elements (in each dimension) are of particular interest.

The second section aims at capturing the user's level of GDPR understanding to determine their actual data sharing behavior. These insights will be benchmarked against the willingness to share such data[3] and thus used for validation purposes. Within the section, the privacy preferences will be assessed as well. The results of the first section thereby make it possible to measure the average level of privacy awareness and expertise of individuals. Thus, the legal factors will be quantifiable. This prerequisite facilitates a detailed assessment of subsequent answers and indicates the basic preferences a privacy interface should consist of.

The third section evaluates psychological factors to determine the inherent level of trust, respectively, the distrust of users towards organizations as well as a detailed examination of trustworthiness-building dimensions and factors. In order to examine the psychological factors in-depth, the survey further provides a range of colors from which participants can select one that they associate with trustworthiness, which has a positive effect on the emotions. The collected data aims at identifying statistically significant relationships among psychological factors and their effect on the overall satisfaction of privacy control. This is particularly interesting, because users' active control over their data is limited, as identified in the underlying doctoral dissertation.

The fourth section's primary focus is on the in-depth evaluation of privacy control elements by evaluating statements that involve assessing parameters that would improve trustworthiness and the evaluation of the personal privacy cockpit interface. The collected data will be used to analyze the privacy preferences and benchmark them against their actual behavior. The data will also be used to validate existing research results. Both internal and external validation strengthens the significance of the gathered data. An example for external validation involves a question regarding the time spent reading a privacy policy, which will be benchmarked against how long it takes to really read one, based on the research article The Cost of Reading Privacy Policies (Mcdonald & Cranor, 2008).

Free text space is further integrated at the end of the survey for additional insights and wishes for enhancing the privacy control as well as feedback on the survey quality. This is

[3] Questions will be asked in different sections.

assessed through Text iQ, a built-in natural language processing service provided by Qualtrics.

4.2. Data Collection Process

A total of 431 participants have completed the survey, whereas roughly 90% of responses are collected via Google Forms and remaining 10% via Qualtrics. The higher engagement on Google Forms is possibly due to the distribution of the survey via different social media platforms. There are 84 possible answers per submitted survey in total. Four of them, incl. the country of residence, age group, occupation, and gender, are mandatory. These obligatory demographic questions facilitate a better evaluation of the audience's contextual aspects. About 7.6% of all 84 questions (incl. the mandatory) are left blank, i.e., 2745 out of 36120 individual answers. The majority of questions have been kept non-compulsory, as this measure has been implemented to ease the answering procedure.

Although users can respond with "0", which indicates that the specific person does not own a device, some responses have not provided any answer at all. A listwise deletion (Saunders et al., 2006, p.21), i.e., removing entire answers from the dataset will not be considered, as it reduces the sample size and consequently loss of representativeness and meaningfulness of the data. Replacement of blank cells with mean values does not occur, as the standard deviation will be slightly reduced and thus introduce bias in the observed data. Either way (replacing or not replacing) preserves the mean as well as the entire range of values, incl. outliers. Another factor speaking against a replacement of blanks with the means is the existence of categorical values for which it is not possible to determine the mean. This would require the application of different methods to eliminate blanks.

Hotdecking (Saunders et al., 2006, p.21) is a possible solution as it identifies respondents with similar answers and replaces the missing values where answers are incomplete. Since the data is equally distributed among different genders, age groups or occupations and the required effort to develop a respective algorithm to deal with the multitude of answers (36.120 individual answers), a more pragmatic solution will be used. A combination of the Index and Randbetween function is applied to generate data from the existing reference distribution rather than having Excel randomly select values from a random range (Fish et al., 2017, p.86). The model would generate a value for categorical and numerical data based on a uniform distribution irrespective of the data type. Therefore, the frequency of existing data is largely maintained, while some noise may be added, represented by the relative percentage difference column in the table below.

Table 1 shows the distribution for observed and generated values of the answers for "Please indicate the type and number of devices you own as well as if it is a personal or shared device [SmartTV]". Please note that the table below only shows the frequency of Smart TV's and not whether it is a personal or shared device.

Table 1: Exemplary Comparison of Observed and Generated Data

Value	Observed	% of total	Generated	% of total	Relative Change
0	77	24.37%	30	25.00%	-0.63%
1	220	69.62%	82	68.33%	1.29%
2	19	6.01%	8	6.67%	-0.65%
3	0	0.00%	0	0.00%	0.00%
Sum	316	100%	120	100%	0.00%

In the table above, 120 blank cells have been replaced with randomly generated values. For quality assurance, this test has been conducted on columns with fewer and more blank cells. The outcomes for both observed and generated data show similar results.

In the scope of the data collection process, there are non-controllable parameters worth mentioning. The Qualtrics results provide a start and end date feature, from which the time spent to complete the survey is calculated. The mean time is 18 minutes, whereas the fastest response time is ≤ 3 and the longest 51 minutes. However, as this sample size accounts for 10% of all responses, it cannot be ruled out that all observations deviate from that.

There is further the risk of possible bots, also known as automated form fillers (Buchanan & Scofield, 2018, p.2588). These bots can easily be installed as a plugin. They randomly select answers on behalf of the respondent, resulting in lower data quality and lack of representativeness. The Qualtrics page timer measures the time between the first and last click (Buchanan & Scofield, 2018, p.2589), whereas no clicks are not recorded. Based on the Qualtrics responses, there are 16 responses between 0 and 3 minutes. The threshold is determined by assessing the response quality and quality, whereas all respondents who spent 4 or more minutes have fully answered on average 70 of 84 questions and below the 4 minutes mark 5 of 84 questions. In fact, the data shows that most of the responses given between 4 and 30 minutes till full completion have the highest response rates.

Comparison with Google Form responses shows that Qualtrics users answer an average of 7.6 fewer questions. All the responses below the threshold show similar behavior, i.e., they answer the first few questions and skip the remaining ones for the sake of completion. This does not simulate the behavior of the bot. The data shows clearly that the survey participants instead discontinued. Thus, it can be ruled out that bots were used, as there is no indication of high response frequency and provided within the 3 minutes threshold. Random responses are another issue the data quality may suffer from, and that is not controllable. A countermeasure to limit such cases is the placement of the survey on specific platforms to target various individuals while preserving a representative dataset.

For all Google-based responses that account for 90% of all collected responses, it is not feasible to limit responses to one per user, since that would require users to log in to Google accounts. As this is not purposeful, it was decided against it. The evaluation of the

timestamps, however, does not show any conspicuous events. It will be therefore assumed that no one has completed the survey more than once[4]. In summary, the methodological approach presented the set up for the data collection and the framework of the underlying survey.

Different measures for data extraction and transformation, as the prerequisite stages for the subsequent analysis, have been compared and assessed based on their effectiveness for this research. The underlying data quality is presented and analyzed transparently and provided by understanding the consequent analysis for the readers. Moreover, not controllable parameters are identified, and their effects on the data are discussed.

4.3. Conclusion of Paragraph

The purpose of this chapter was to drill down into the data, to analyze and evaluate the insights with respect to the identification of elements and features that increase control over data, improve trustworthiness of organizations and ultimately conclude data-driven features for the conceptualization of a user centric privacy control system.

The results are manifested in the 3D concept of trustworthiness building factors (see figure 2). The approach was to progressively evaluate the elements from the cube in a target-oriented method. Essential results are documented during this summary, while the detailed evaluation of this chapter is contextualized in conjunction with overall analysis results of this research undertaking.

A key insight – based on a broader view on the data and irrespective clusters – is that users have a limited transparency over their processed data, as they spend insufficient time understanding underlying processing activities. A countermeasure was identified in the scope of the necessity of certifications. It is arguable that certifications serve effectively as a trust building element that can be used to reduce the gap in understanding of technologies and processes deployed by organizations.

However, certificates are not a replacement for independent information searches. There is a residual risk that individuals will rely upon certifications and skip the information search, since a previous analysis (Ider, 2020a, p.108) identified that most individuals merely spend two minutes on a website to familiarize themselves with privacy modalities. This circumstance shows that the combination of trustworthiness building elements may limit or in the worst case cancel out the effectiveness of the respective other measure. The results further identify that organizations need to be more transparent and provide additional information on their processing activities as well as technologies, as these are the two areas where the individual has no power to actively exercise control, i.e., the user right, thus, must depends on the quality and quantity of information provided by the organization[5].

A general conclusion that can be drawn from the observations and thus from users' perspectives is that respondents understand and differentiate between different categories of

[4] Also, with the consideration that respondents seek to increase their chances of winning an amazon gift voucher.
[5] See Figure 16 for details, color scale used to highlight users' active power to exercise control over their data.

personal information. The survey participants seem to be more conservative and less willing to trade off their sensitive data, while they are more comfortable sharing non-sensitive data for fewer rewards.

A detailed view on the clustered segments further allowed the narrowing down and specifying of elements of trustworthiness building factors. Preferably, features that reduce the search for information are information access, transparency of data processing and use of plain language, which facilitate easy comprehension and drill down into privacy information. This is a way to improve engagement with policies and meet user behavior.

The analysis accentuated the elements that are of higher importance for the users in the context of engagement with privacy modalities of organizations. Accordingly, the research results revealed that users prefer less plain text, but rather easier obtainable blocks, organized in subtopics and supported by interactive icons and videos, which improve the understanding of the content.

Further, accessibility to personal data is strongly associated with a higher control perception and thus, increase in trustworthiness. Such access is facilitated through a simplified user interface navigation, which requires fewer but selected functionalities.

Contrary to the trustworthiness creating features presented above, links to fan pages (e.g., Facebook, Twitter, Instagram) neither affect the users' perception of psychological control over data nor change trust in a meaningful way. This question served two purposes, firstly, to find out whether users effectively differentiate between links to fan pages and certifications of official bodies (e.g., EDPS, ICO, ISO, NIST) and secondly, to evaluate the effects of fan pages on the development of trustworthiness of organizations. Clearly, a major gap that has been identified with regards to the improvement of control and trustworthiness is the low level of user engagement with privacy modalities of organizations. Yet, the need for stronger engagement and improvement of privacy awareness is considered a high priority for individuals. This shows that there is a contradiction between the attitude and the actual behavior of users, which strengthens Kokolakis' findings in the scope of the privacy paradox phenomenon study (2017, p.124).

The validation of the attitude versus behavior dichotomy has been carried out through questions that required users to actively engage with a mockup PPC user interface, while other sets of questions were targeted to capture the attitude. Comparing the results of preceding analyses, it can be concluded that in hypothetical set ups, i.e., assessments of the self-reported (attitude) rather than observed (behavior), users tend to be more optimistic about their abilities and behaviors towards exercising their user rights, while the measurement of actual behavior shows evidence of lower confidence. In terms of actual Figures, the dichotomy delta is at 32%, i.e., the attitude is rated about ⅓ higher than the actual behavior.

Information and data access as well as the exercise of data erasure show the highest discrepancy, with an average delta of 64%. Hence, an implementation of a central privacy control system for users would significantly reduce the delta resulting from the dichotomy.

Lastly, only 5% of all respondents provided their email address to participate in the raffle. The validation of the data for the purpose of the dichotomy assessment of respondents does not deviate from the remaining 95% and is therefore not conclusive and significant for this research.

In summary, the chapter provided detailed evidence for the elements of the trustworthiness building factors. It further facilitated the quantification and assessment of such features for the improvement of data control as well as the establishment of trustworthiness of organizations. It has been identified that behavioral perception strongly deviates from actual behaviors and that legal as well as technological control over data, processes and IT systems play a subordinate role and are strongly influenced by attitudes of survey participants.

4.4. Chapter Summary

- Scope:
  - This chapter focuses on the methodology used for collecting and analyzing data on users' and organizations' trustworthiness-building factors.
- Methods:
  - An international web-based survey was conducted in March and April 2021 using Qualtrics and Google Forms. The survey consisted of 25 questions with 84 subcategories, clustered into four sections, aimed at capturing users' privacy awareness and expertise, trust towards organizations, evaluation of privacy control elements, and feedback on the survey quality.
- Results:
  - The majority of the responses were collected via Google Forms (90%) compared to Qualtrics (10%). The results aimed to measure the average level of privacy awareness, benchmark privacy preferences against actual behavior, validate existing research results, and determine trustworthiness-building factors.
- Novelty:
  - The results provide insights into users' privacy awareness and behavior, and their trust towards organizations, which will inform the development of a user-centric privacy control system.
- Conclusion:
  - The chapter outlines the data collection and analysis methodology used in the study. The results provide insights into users' privacy awareness and behavior, and their trust towards organizations, which will inform the development of the user-centric privacy control system.

5. Chapter: Experimental Verification

In the Conclusion section of the scientific dissertation, the main findings of the study are summarized and interpreted comprehensively in the context of the research questions and hypotheses. Significant trends and patterns are identified, contributing to the current understanding of the field. The implications of these findings are discussed, including their significance for the development of new theories and practices, and potential avenues for future research are identified. Reflections are made on the limitations of the study and the methodological or theoretical contributions of the research, which may inform future work in the field.

5.1. Research Findings

The comparison of the adaptation probabilities of the peer privacy systems (see Figure 1) proposed an entry strategy that decreases the technical burdens for the implementation of the envisaged privacy control system. The upside of such a strategy is the elevation of operational feasibility, ensured through privacy by design measures such as the hosting of service and data storage set up within the EU, a centralized development and maintenance of the interface and ease of facilitation through API connectivity interfaces. Smaller or less technologically capable organizations without the necessary competencies and resources may however struggle to connect to such a system.

Secondly, the actual conditions of organizational privacy maturity cannot be verified and thus, constitutes a limitation in the research that must be critically appraised. Despite the assessment of external research results as well as comprehensive market studies with regards to the maturity of GDPR compliance across organizations, the true condition is not fully reflectable. This circumstance is important to consider as it will influence the success and operationalizability of the proposed privacy control system. It will further affect the trustworthiness of organizations, as the conceptualized framework for the evaluation of trustworthiness is partially based on the maturity of organizational GDPR compliance. During this research a partial offsetting of the uncertainty of the circumstances could have taken place through external certification mechanisms.

Thirdly, limiting the length of a privacy policy is considered by survey respondents a necessity to improve effective compliance and further build trustworthiness as well as improve data control. However, the reduction of policy content could be counterproductive as it limits the space for organizations to meet their accountability requirements for their processing activities. In a wider scope, this leads to an increased difficulty for organizations to reflect the privacy modalities transparently. This is particularly critical as the trend shows that the introduction of new and additional processing activities of personal information, i.e., extension of use cases, entails an enlargement of the policy text. This circumstance may increase the difficulty to keep policies short while reflecting the operations in a comprehensive manner.

Lastly, in the view of some organizations, it is the ultimate responsibility of the individual to thoroughly examine the privacy modalities (Mcdonald & Cranor, 2008, p.568). However, this research proved that there is a great responsibility and thus obligation on the part of organizations to facilitate a user-friendly interface and highlight specific design feature requirements that improve engagement with privacy modalities to ultimately improve users' data control and trustworthiness. Even greater significance is attached to the impact of the regulators, as they function as a binding force between organizations and individuals. Thus, a critical success factor for effective privacy compliance is the speed and timing of regulators to pass legislations.

If organizations resist or even fail to meet their accountability requirements with regards to data protection, regulators must step in and intervene to ensure effective compliance. The research of the operational feasibility highlights the necessity of a symbiosis of regulations and organizational compliance efforts to promote operationalization of the GDPR and ultimately achieve effective privacy compliance through better user engagement. Critical success factors are the underlying organizational capabilities and resources as well as the timeliness of implementation of measures. In the developed privacy construct, the least controllable and most challenging parameter identified is the true maturity condition of organizations. The dissertation not only provided the legal assessment and requirements, but also laid down the basis for the technical control analysis. Main takeaways of the legal control assessment are the identification and differentiation of user rights that can be actively and passively exercised. In this scope a segmentation of user rights by level of importance was provided, which led to the specification of features for the control system and UI specifications, i.e., better visibility and easier access for higher rated rights.

The technical control has manifested in the effective initialization of the legal criteria, including and in particular the exercise of user rights by individuals as well as the enablement of organizations to comply with the legal standards through privacy by design guidelines that allow organizational control on an operational (business process) and information system level. Consequently, the analysis provided explicit guidance for the implementation of the system that is consistent with the legal requirements.

The evaluation of psychological control has shown that the control perception across various dimensions strongly correlates with the provisioning of a simple user-friendly UI and UX. An essential discovery is the reduction of the time cost for reading policies. There is an extreme dichotomy between the actual time spent on reading policies and thus time spent on privacy modalities versus the time needed to fully read such policies. Latter does not measure or imply the level of understanding but merely the time spent reading. The existence of the gap between self-reported and observed behaviors that have been analyzed in an external study has been validated in the scope of a survey conducted for this dissertation[6].

[6] The implementation of time-reducing features is derivable from the legal and technical assessment results and has been listed by importance in the preceding analysis.

Therefore, an initial step in the improvement of control and trustworthiness is the decrease of the burden for information search and the associated time cost for accessing and processing such information. The assessment highlighted that the user experience, i.e., perception of privacy modalities, its presentation, content, length, interface design and navigation essentially influence the time cost.

A distinctive characteristic of psychological control perception is its impact on user behavior. While legal and technical aspects can be considered as external enablers or channels for effectively implementing control features, psychological control is the judgment of an individual of ultimate power or influence over their own personal information held in the possession of a third party.

This in turn affects the trustworthiness of the third party as trustworthiness is the degree of certainty, resp. openness of users towards organizations to share their data. While users' inherent perception for data sensitivity is a key contributor to willingness and frequency for data sharing, it was observed that based on their level of control they can exercise over their own data, the confidence and readiness to share data increases, irrespective of the data type.

Additionally, to better understand the psychological behavioral patterns of users, color influences on trustworthiness were analyzed. It was found that user trust in organizations can be actively and more strongly influenced by certain colors than by other colors. Almost every second participant stated that the color blue has the strongest trust-building effect, followed by green, true for 25% of participants. Such colors decrease the risk aversion and directly impact the users state of feelings, i.e., promoting relaxation and reducing distress while parallelly improving trustworthiness. In order to maintain the corporate identity, it has been further suggested to apply trust-building colors solely to the centralized privacy control system. Considering the identified findings as well as their interactions, the psychological effects can be assigned a higher weighting than the legal and technical control perception for achieving effective trustworthiness. Ultimately, a user-friendly complexity-reducing control system that facilitates the reduction of the time cost, the improvement of individual judgment capabilities associated with effective exercise of rights as well as the usage of specific colors for the interface manifested in the symbiosis of legal, technical, and psychological features leads to an effective control and improvement of trustworthiness.

5.2. Requirements Specification of System Modules

The modules for the control system have been derived from the privacy cube (figure 2). They refer to the features built into the control system that aim to effectively enhance trustworthiness from a user perspective. Based on these evaluated features, privacy control attributes have been derived.

This process facilitated the modeling of a chain of dependencies and their causal relationships among sub-segments and across the various crosstab areas. The cube, set up as a

multidimensional crosstab, splits the organization (x-axis), control (y-axis) and the segmentation criteria (z-axis). The x-axis is broken down into data, processes and IT systems and the y-axis into psychological, legal, and technological control elements. The z-axis is subdivided into age group, occupation, and device usership. Each crosstab area consists of defined assessment parameters, which were directly represented in the survey. The analysis results identified that the legal framework (figure 3) functions as the juridical backbone for the exercise of user control. It is the interface between users and organizations and therefore has the highest impact, as small changes in legal requirements affect all subsequent aspects of the cube and consequently the control over data from a user perspective.

In consideration of the nature of business operations they determine the processing (usage), retention and deletion of the data.

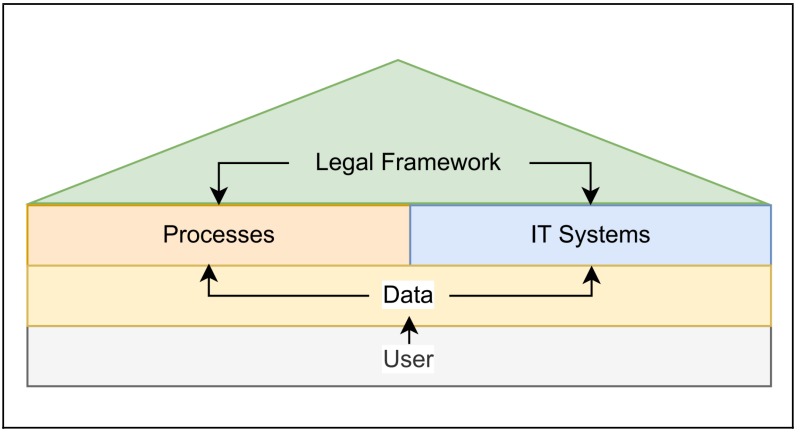

Figure 1: Simplified Composition of Relevant Subject Matter Symbiosis

Essentially, the technological resources driving the processing of data can only take place upon predetermination of legal boundaries, substantially expressed in the privacy policy of an organization. The legal boundaries are always immediately in compliance with the GDPR, while processing activities vary based on the nature of business operations. Achieving a consistent synchronization of both, the legal requirements, and operational activities, is the greatest challenge for organizations according to the results of this research. In addition, psychological control perception is the vital key factor that needs to be supported by technology enablers. The privacy triad, represented by the three pillars legal, user and organization[7] for effective privacy control and establishment of organizational trustworthiness. If this foundation is not given, the exercise of effective control is not achievable to an adequate extent.

[7] Organization comprises data, processes, and IT systems in figure 2.

5.3. Applicability of research concept

The preceding synopsis highlighted the design features for the privacy user interface. In principle, the control system serves a mediatory function, as it leads to an increase in user engagement with organizations, which is reflected in the increased willingness to share personal data.

In addition to identifying features that promote effective control, the aggregation of control modules resulted in the selection of areas to be described in detail, as well as the scope of the content and the aspects that should be made more explicit. These measures increase the interface characteristics of the control system. Furthermore, a dichotomy between self-disclosures and observations in terms of engagement with privacy practices was identified, which is mitigated by improved and more accessible features that facilitate better engagement with privacy systems. Easy access to technical and organizational security measures is also an additional measure that facilitates user understanding. As a result, effectively relevant privacy content is included, and better understanding is achieved, thus further validating the applicability of the research concept.

This insight confirms findings of a reference research, which shows that a control system establishes and improves corporate trustworthiness (Coletti et al., 2005, p.479).

Beneficiaries of the system are both individuals as well as organizations. Both parties are either the immediate contributors of the resource, i.e., users provide personal information or are the ultimate beneficiary of such data, i.e., organizations consuming the data. In the latter case, compliance and accountability requirements arise and will be met by implementing the privacy control system. Both interest groups share the output, i.e., product or service, either used or produced, as a common feature. The individuals are the primary beneficiaries, as the privacy control system will be designed for the improved control of personal information in the first place. The primary institutional beneficiaries are all data protection officers of the European Union. They may use this concept as a blueprint to implement measures for improving GDPR compliance. Moreover, the private sector is a potential target as well. Particularly, industries affected by fines (for non-compliance with the GDPR) are of most interest. Figure 3 below shows the accumulated proportional penalties imposed on the industries until December 2020[8].

[8] The industries are segmented according to predefined labels provided by the reference source.

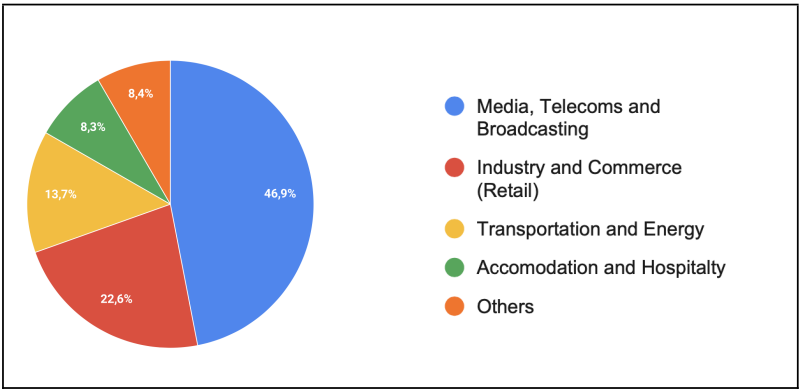

Figure 2: Proportions of Industries Affected by GDPR Fines (Ider, 2020b).

The incentive for organizations to connect to the privacy control service is its increased transparency, enhancing its GDPR compliance by effectively disclosing the personal information of individuals more straightforwardly and comprehensively. Ultimately, such engagement should also be recognized and acknowledged by European Data Protection Officers in case of violations, resulting in decreased fines for participating organizations as they can demonstrate their efforts to meet their accountability obligations.

5.4. Future Development

One of the main research outcomes is the development of a proof of concept for an online privacy control system. The further research stage should involve the prototyping and testing of a workable model. The identified control features shall be adjusted accordingly in a subsequent cycle. Alongside the testing of the prototype, researchers should measure if the dichotomy with regards to the self-reported and observed values can be narrowed down or even closed. This procedure enhances the quality of the data by matching self-reported and researcher-recorded information, thereby reducing uncertainties about the data.

Although the development and establishment of the GDPR law is a result of European joint efforts, among the various supervisory authorities, there are significant differences in the provisioning of best practices, guidelines, and monitoring activities. Conversely, studies show strong variations in the de facto enforcement of fines or prosecution in the event of data protection violations. As a result, it appears that EU member states lack a common consensus regarding their data protection practices and further collaboration with organizations. Consequently, this circumstance decreases the incentive to implement a user privacy control system, where active regulatory supervision efforts through and/or penalty enforcement is low. Hence, it is recommended that the authorities increase their cooperation with the private

and public sector. On the other hand, imposing penalties should be consistent with the efforts that jurisdictions undertake to promote data protection compliance. After all, the regulatory system is an integral contributor to the success of effective data protection.

With further reference to the commitments of supervisory authorities, they should form a task force for researching user needs in the interaction with privacy modalities. In addition, organizational challenges shall be adequately addressed in resources published or provided by the authorities to promote effective GDPR implementation. Such measures will enhance the ability of government agencies to improve their function as a link between individuals and organizations. Ultimately, this will benefit users through increased control over their data and companies through improved trustworthiness. Other areas of privacy research should take place in the determination of a framework for measuring the level of consciousness, transparency, comprehensibility, easy access to information and guidelines for clear language. Particularly the ability to measure complexity respectively, ease of the language is a determinant for users to establish and increase trust as well as further control. The ultimate goal for the recommended research area shall promote the power of the individual user to control their personal data more actively and counteract the increasing trend of control shifting to data processing organizations.

5.5. Chapter Summary

- Introduction:
  - The study aimed to propose an entry strategy for a privacy control system
  - Goal was to decrease technical burdens and elevate operational feasibility
- Methodology:
  - Legal, technical, and psychological control were integrated in the analysis
- Results:
  - Study showed strong correlation between user-friendly UI/UX and its impact on user behavior and trustworthiness
  - Shortening of privacy policy deemed necessary but could limit transparency
  - Importance of reducing time cost for information search and impact of user experience on privacy and trustworthiness highlighted → rearrangement and displaying of privacy rights
- Novelty:
  - The study provides insights into the users' level of privacy awareness and expertise, trust towards organizations, evaluation of privacy control elements, and feedback on survey quality (through internal and external data validation methods).
  - The results also validate existing research results and determine trustworthiness-building factors.

    - Proposed system will empower individuals to control their personal data
    - Countering the trend of control shifting to data processing organizations
- Limitations:
    - Validation of organizational privacy maturity through evaluation of secondary sources
    - Organizations ultimately responsible for facilitating user-friendly interface to improve data control and trustworthiness
- Future Development:
    - Prototype development and testing to reduce dichotomy between self-reported and observed values
    - Increase cooperation between supervisory authorities, private, and public sector for consistent penalties for data protection violations

6. Approbation

Delivery Hero SE intends to adopt a more user-centric approach to their privacy control system to foster trust and confidence with their customers. To achieve this, they plan to integrate the research results into their business processes to simplify their GDPR compliance and streamline their privacy control system. By applying the research findings to their existing system, they aim to evaluate its effectiveness and identify areas for improvement. Ultimately, the company seeks to enhance their reputation and build trust among their customers by ensuring robust privacy and data protection measures.

7. Conclusion

This scientific study focuses on developing a user-centric privacy control system that aids organizations in complying with the General Data Protection Regulation (GDPR) by considering societal impact, fuzzy regulations, and technology. The study highlights the importance of reducing technical burdens and providing a user-friendly interface to improve users' data control and trust. The proposed privacy control system empowers individuals to control their personal data, which counters the trend of control shifting to data processing organizations. The study suggests that there is a great responsibility and obligation on the part of organizations to facilitate a user-friendly interface and regulators to ensure effective compliance.

The methodology of the study includes surveys, systematic literature review, and a design thinking process. An international web-based survey consisting of 25 questions and 84

subcategories clustered into four sections was also conducted to understand user privacy awareness, trust towards organizations, evaluation of privacy control elements, and feedback on the survey quality. The results of the survey show a strong correlation between user-friendly UI/UX and impact on user behavior and trustworthiness. The study also highlights the importance of reducing the time cost for information search and the impact of user experience on privacy and trustworthiness.

The study identifies limitations such as the inability to verify organizational privacy maturity and suggests future developments, including prototype development and testing, cooperation between supervisory authorities, private and public sectors, and a task force to research user needs and organizational challenges. The goal is to enhance individual control over personal data and promote trust between individuals and organizations. The reduction of policy content to improve compliance and build trustworthiness could be counterproductive as it limits the space for organizations to meet their accountability requirements. Overall, the study provides explicit guidance for the implementation of the privacy control system that is consistent with legal requirements, which can improve the perception of control and trustworthiness.

8. Research Contributions And Advances

This scientific study presents a novel unified framework for GDPR compliance, which simplifies the implementation process for organizations and improves user control over their personal data through a privacy control system. The research provides insights into users' privacy awareness, trust towards organizations, evaluation of privacy control elements, and feedback on survey quality using internal and external data validation methods. The proposed system empowers individuals to control their personal data, counteracting the trend of control shifting to data processing organizations. The study highlights the importance of considering societal impact, fuzzy regulations, and technology in evaluating organizational trust and reveals the impact of control over personal data, processes, and systems on trustworthiness. Overall, the study brings a practical and novel approach to the current challenges in GDPR compliance.

9. Applied Research Contributions

The research study utilizes two web applications, Qualtrics and Google Forms, to conduct an international web-based survey to assess users' privacy awareness, trust towards organizations, evaluation of privacy control elements, and feedback on survey quality. Qualtrics is an online survey software that enables users to design and distribute surveys and analyze responses, while Google Forms is a free web-based survey tool that enables users to create surveys and collect responses in real-time.

The study also employs a web scraper to collect over a thousand fines, which are analyzed and contextualized to identify trends in GDPR compliance. The web scraper is self-designed and developed to extract data from websites, enabling the collection of relevant information to the research. By utilizing these web applications and the web scraper, the study is able to gather and analyze data from a diverse range of sources, providing a comprehensive and nuanced understanding of the issues surrounding GDPR compliance.

10. Bibliography

Alford, S. (2020) GDPR: A Game of Snakes and Ladders: How Small Businesses Can Win at the Compliance Game [Online]. 1st ed. Routledge. Available from: <https://www.taylorfrancis.com/books/9781000027150> [Accessed 1 June 2021].

Andreoni, J. & Miller, J. (2002) Giving According to GARP: An Experimental Test of the Consistency of Preferences for Altruism. Econometrica, 70 (2).

Article 29 Working Party (2014) Opinion 05/2014 on Anonymisation Techniques 0829/14/EN [Online]. Available from: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf> [Accessed 16 November 2020].

Article 29 Working Party (2016) Guidelines on the Right to Data Portability [Online]. Directorate C (Fundamental rights and rule of law) of the European Commission, Directorate General Justice and Consumers, B-1049 Brussels, Belgium, Office No MO59 05/35. Available from: <https://ec.europa.eu/newsroom/document.cfm?doc_id=44099>.

Article 29 Working Party (2017) Guidelines on Transparency under Regulation 2016/679 [Online]. Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013. Available from: <https://ec.europa.eu/newsroom/article29/items/622227>.

Ashraf, N., Bohnet, I. & Piankov, N. (2006) Decomposing Trust and Trustworthiness. Experimental Economics, 9 September, pp. 193–208.

Betti, D., Lacey, J. & Dhoni, I. (2020) 6th GLOBAL SMARTPHONE USER SURVEY [Online]. Mobile Ecosystem Forum Ltd. m, p. 9. Available from: <https://mobileecosystemforum.com/wp-content/uploads/2020/05/MEF_Global_Smartphone_Survey_2020_Summary.pdf>.

Buchanan, E. M. & Scofield, J. E. (2018) Methods to Detect Low Quality Data and Its Implication for Psychological Research. Behavior Research Methods [Online], 50 (6) December, pp. 2586–2596. Available from: <http://link.springer.com/10.3758/s13428-018-1035-6> [Accessed 9 April 2021].

Coletti, A. L., Sedatole, K. L. & Towry, K. L. (2005) The Effect of Control Systems on Trust and Cooperation in Collaborative Environments. The Accounting Review [Online], 80 (2) April, pp. 477–500. Available from: <https://meridian.allenpress.com/accounting-review/article/80/2/477/53536/The-Effect-of-Control-Systems-on-Trust-and> [Accessed 3 January 2022].

Colman, A. M. (2003) A Dictionary of Psychology. Oxford: Oxford University Press.

ContentSquare (2020) Digital Experience Benchmark Report 2020 [Online]. p. 7. Available from: <https://go.contentsquare.com/en/digital-experience-benchmark> [Accessed 18 December 2020].

Council of Europe (1981) Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. European Treaty Series No. 108 (108), p. 7.

Dehmel, S. & Kelber, U. (2020) DS-GVO Und Corona – Datenschutzherausforderungen Für Die Wirtschaft (Translation: GDPR and Corona - Data Protection Challenges for Business) [Online]. Bitkom, p. 12. Available from: <https://www.bitkom.org/sites/default/files/2020-09/bitkom-charts-pk-privacy-29-09-2020.pdf> [Accessed 20 December 2020].

Desnoyers, L. (2011) Toward a Taxonomy of Visuals in Science Communication. Technical Communication (Washington), 58 May, pp. 119–134.

DIMITROV, I. (2021) Invasive Apps. The pCloud Blog, 5 March [Online blog]. Available from: <https://blog.pcloud.com/invasive-apps/> [Accessed 6 May 2021].

European Commission (n.d.) Can Individuals Ask to Have Their Data Transferred to Another Organisation? [Online]. European Commission - European Commission. Available from: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/dealing-citizens/can-individuals-ask-have-their-data-transferred-another-organisation_en> [Accessed 3 January 2021a].

European Commission (n.d.) What Constitutes Data Processing? [Online]. European Commission - What constitutes data processing? Available from: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_en> [Accessed 9 July 2021b].

European Data Protection Board (EDPB) (2020) Guidelines 4/2019 on Article 25 Data Protection by Design and by Default [Online]. Available from: <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf>.

Eurostat (2020) Annual Enterprise Statistics by Size Class for Special Aggregates of Activities (NACE Rev. 2) [Online]. Available from: <https://ec.europa.eu/eurostat/databrowser/view/sbs_sc_sca_r2/default/bar?lang=en> [Accessed 23 December 2020].

Faustino-Bauer, M. & Ider, K. (2020) Datenschutzmanagement - Ein Erfolgsfaktor bei der digitalen Transformation (Translation: Data protection management - a success factor in digital transformation). 6 / 2020 December, pp. 247–255.

Federal Ministry for Economic Affairs and Energy (BMWi) (2019) Project GAIA-X – A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem [Online]. Federal Ministry for Economic Affairs and Energy Public Relations. Available from: <https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/project-gaia-x.pdf?__blob=publicationFile&v=4>.

Federal Ministry of Justice and Consumer Protection (2017) Federal Data Protection Act (BDSG) [Online]. p. 43. Available from: <https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.pdf> [Accessed 19 December 2020].

Fish, L. J., Halcoussis, D. & Phillips, G. M. (2017) Statistical Analysis Of A Class: Monte Carlo And Multiple Imputation Spreadsheet Methods For Estimation And Extrapolation. American Journal of Business Education (AJBE) [Online], 10 (2)

March, pp. 81–96. Available from: <https://clutejournals.com/index.php/AJBE/article/view/9918> [Accessed 9 April 2021].

Forsa (2018) Forsa Umfrage: Alles unter Kontrolle?! (Translation: Forsa Poll: Everything under control?!) [Online]. Available from: <https://www.klicksafe.de/ueber-klicksafe/safer-internet-day/sid-2018/forsa-umfrage-alles-unter-kontrolle/> [Accessed 19 December 2020].

General Data Protection Regulation (2016), Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

GDPR Enforcement Tracker - List of GDPR Fines (n.d.) [Online]. Available from: <https://www.enforcementtracker.com> [Accessed 29 May 2022b].

Glossary - EUR-Lex (n.d.) [Online]. Available from: <https://eur-lex.europa.eu/eli-register/glossary.html> [Accessed 9 July 2021c].

Grashöfer, J., Degitz, A. & Raabe, O. (2017) User-Centric Secure Data Sharing: Exploration of Concepts and Values. [Online]. Available from: <https://dl.gi.de/handle/20.500.12116/3888> [Accessed 30 September 2020].

Gul, F. A. (1983) A Note on the Relationship between Age, Experience, Cognitive Styles and Accountants' Decision Confidence. Accounting and Business Research, 14 (53) December, pp. 85–88.

Haas, A., Wagner, C., Miyashita, G., Hall, K., Fiorillo, C., Heath, J., Gol, H., McDougal, T., Huggins, K., Laurenza, A., Small, R., Orkin, S., Rayment, S., Byrne, Y., Datwani, H., Campos, F., O'Brien, C. & Emerson, T. (2019) Global Contact Center Survey [Online]. p. 16. Available from: <https://www.deloittedigital.com/content/dam/deloittedigital/us/documents/blog/blog-20190513-2019%20globalcontactcentersurvey.pdf> [Accessed 16 April 2021].

Ider, K. (2020a) Effective Privacy Management Concepts: Increasing Privacy Control by Reducing Complexity. vol. 24. Berlin: Shaker Verlag GmbH, pp. 103–110.

Ider, K. (2020b) based on data from Enforcementtracker.com. (n.d.) GDPR Enforcement Tracker - List Of GDPR Fines. [online] Available from: <https://www.enforcementtracker.com/> [Accessed 12 December 2020].

Jiang, Z., Tolido, R., Jones, S., Hunt, G., BUDOR, I., Bartoli, E., Linden, P. van der, Buvat, J., Theisler, J., Wortmann, A., Cherian, S. & Khemka, Y. (2019) Championing Data Protection and Privacy – a Source of Competitive Advantage in the Digital Century [Online]. Available from: <https://www.capgemini.com/de-de/wp-content/uploads/sites/5/2019/09/Report_GDPR_Championing_DataProtection_and_Privacy.pdf> [Accessed 18 August 2020].

Joint Task Force Transformation Initiative (2013) Security and Privacy Controls for Federal Information Systems and Organizations [Online]. NIST SP 800-53r4. National Institute of Standards and Technology, p. NIST SP 800-53r4. Available

from: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf> [Accessed 14 December 2020].

Kemp, S. (2020) Digital 2020: Global Digital Overview [Online]. DataReportal – Global Digital Insights. Available from: <https://datareportal.com/reports/digital-2020-global-digital-overview> [Accessed 13 November 2020].

Kerkhof, P. & Noort, G. (2010) Third Party Internet Seals: Reviewing the Effects on Online Consumer Trust. Encyclopedia of E-Business Development and Management in the Global Economy, 2 January.

Kissel, R. L. (2013) Glossary of Key Information Security Terms. U.S. Department of Commerce.

Kokolakis, S. (2017) Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon. Computers & Security [Online], 64 January, pp. 122–134. Available from: <https://linkinghub.elsevier.com/retrieve/pii/S0167404815001017> [Accessed 14 December 2021].

Lintvedt, M. N. (2021) Putting a Price on Data Protection Infringement. International Data Privacy Law [Online], December, pp. 1–15. Available from: <https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipab024/6453860> [Accessed 17 January 2022].

Lyons, J. B., Stokes, C. K., Eschleman, K. J., Alarcon, G. M. & Barelka, A. J. (2011) Trustworthiness and IT Suspicion: An Evaluation of the Nomological Network. Human Factors [Online], 53 (3) June, pp. 219–229. Available from: <https://doi.org/10.1177/0018720811406726> [Accessed 23 December 2020].

Mcdonald, A. M. & Cranor, L. F. (2008) The Cost of Reading Privacy Policies. I/S: A Journal Of Law And Policy, 4:3, pp. 544–568.

Ministry of Communications and Information (2014) Personal Data Protection Regulations 2014 [Online]. vol. Y03.002.001.EV30/13; AG/LLRD/SL/227A/2012/4 Vol. 2. Ministry of Communications and Information Singapore. Available from: <https://sso.agc.gov.sg/SL/PDPA2012-S362-2014?DocDate=20200528>.

Monteiro, A. F. (2019) First GDPR Fine in Portugal Issued against Hospital for Three Violations. 13 January [Online blog]. Available from: <https://iapp.org/news/a/first-gdpr-fine-in-portugal-issued-against-hospital-for-three-violations/> [Accessed 17 January 2022].

National Institute of Standards and Technology (2006) Minimum Security Requirements for Federal Information and Information Systems [Online]. NIST FIPS 200. Gaithersburg, MD: National Institute of Standards and Technology, p. NIST FIPS 200. Available from: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf> [Accessed 19 December 2020].

Osmanoglu, T. E. (2013) Identity and Access Management: Business Performance through Connected Intelligence. Amsterdam, [Netherlands]: Syngress, an imprint of Elsevier.

Pancer, E., McShane, L. & Noseworthy, T. J. (2017) Isolated Environmental Cues and Product Efficacy Penalties: The Color Green and Eco-Labels. Journal of Business Ethics, 143 (1) June, pp. 159–177.

Personal Information Protection Commission (2016) Amended Act on the Protection of Personal Information (Tentative Translation) [Online]. Japan. Available from: <https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf> [Accessed 26 December 2020].

PricewaterhouseCoopers (2018) Aktueller Stand zur Umsetzung der EU-DSGVO bei Leasinggesellschaften in Deutschland (Translation: Current status on the implementation of the EU GDPR at leasing companies in Germany) [Online]. PwC. Available from: <https://www.pwc.de/de/finanzdienstleistungen/leasing/aktueller-stand-zur-umsetzung-der-eu-dsgvo-bei-leasinggesellschaften-in-deutschland.html> [Accessed 18 August 2020].

Qualtrics.com (n.d.) Response Quality [Online]. Available from: <https://www.qualtrics.com/support/survey-platform/survey-module/survey-checker/response-quality/> [Accessed 26 March 2021].

Rotter, J. B. (1980) Interpersonal Trust, Trustworthiness, and Gullibility. American Psychological Association, 35 (1) January, pp. 1–7.

Ruud, T. F. (2003) The Internal Audit Function : An Integral Part of Organizational Governance. In Bailey, Andrew; Gramling, Audrey & Ramamoorti, Sridhar (Ed.): Research Opportunities in Internal Auditing. Altamonte Springs : IIA-The Institute of Internal Auditors, pp. 73–96.

Sambra, A. V., Mansour, E., Hawke, S., Zereba, M., Greco, N., Ghanem, A., Zagidulin, D., Aboulnaga, A. & Berners-Lee, T. (n.d.) Solid: A Platform for Decentralized Social Applications Based on Linked Data. p. 16.

Saunders, J. A., Morrow-Howell, N., Spitznagel, E., Dore, P., Proctor, E. K. & Pescarino, R. (2006) Imputing Missing Data: A Comparison of Methods for Social Work Researchers. Social Work Research [Online], 30 (1) March, pp. 19–31. Available from: <https://academic.oup.com/swr/article-lookup/doi/10.1093/swr/30.1.19> [Accessed 9 April 2021].

Sjöberg, M., Chen, H.-H., Floréen, P., Koskela, M., Kuikkaniemi, K., Lehtiniemi, T. & Peltonen, J. (2017) Digital Me: Controlling and Making Sense of My Digital Footprint [Online]. In: Gamberini, L., Spagnolli, A., Jacucci, G., Blankertz, B. & Freeman, J. ed., Symbiotic Interaction. vol. 9961. Cham: Springer International Publishing, pp. 155–167. Available from: <http://link.springer.com/10.1007/978-3-319-57753-1_14> [Accessed 1 October 2020].

Skinner, M. (2013) Emotional Control [Online]. In: Gellman, M. D. & Turner, J. R. ed., Encyclopedia of Behavioral Medicine. New York, NY: Springer New York, pp. 671–673. Available from: <https://doi.org/10.1007/978-1-4419-1005-9_950>.

Sobers, R. (2020) How Privacy Policies Have Changed Since GDPR. Inside Out Security, 295T15:07:08-04:00 [Online blog]. Available from: <https://www.varonis.com/blog/gdpr-privacy-policy/> [Accessed 7 May 2021].

Statistisches Bundesamt (Destatis) (2020) Bevölkerung Und Erwerbstätigkeit - Haushalte Und Familien, Ergebnisse Des Mikrozensus (Translation: Population and Employment - Households and Families, Results of the Microcensus) [Online]. Statistisches Bundesamt (Destatis), pp. 43–52. Available from: <https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Bevoelkerung/Haushalte-Familien/Publikationen/Downloads-Haushalte/haushalte-familien-2010300197004.pdf?__blob=publicationFile>.

Su, L., Cui, A. & Walsh, M. (2019) Trustworthy Blue or Untrustworthy Red: The Influence of Colors on Trust. Journal of Marketing Theory and Practice, 27 July, pp. 269–281.

Sutter, M. & Kocher, M. G. (2007) Trust and Trustworthiness across Different Age Groups. Games and Economic Behavior [Online], 59 (2) May, pp. 364–382. Available from: <https://linkinghub.elsevier.com/retrieve/pii/S0899825606001199> [Accessed 19 June 2022].

Truong, N. B., Sun, K., Lee, G. M. & Guo, Y. (2020) GDPR-Compliant Personal Data Management: A Blockchain-Based Solution. IEEE Transactions on Information Forensics and Security, 15, pp. 1746–1761.

Ustaran, E. ed. (2019) European Data Protection: Law and Practice. Portsmouth, NH: an IAPP Publication, International Association of Privacy Professionals.

VandenBos, G. R. ed. (2015) APA Dictionary of Psychology (2nd Ed.). Washington: American Psychological Association.

Vaske, H. (2022) European Cloud Project Gaia-X Is Stuck in the Concept Stage [Online]. CIO. Available from: <https://www.cio.com/article/308818/european-cloud-project-gaia-x-is-stuck-in-the-concept-stage.html> [Accessed 1 May 2022].

Voigt, P. & Bussche, A. von dem (2017) The EU General Data Protection Regulation (GDPR). Cham: Springer International Publishing.

Wasaya, A., Saleem, M. A., Ahmad, J., Nazam, M., Khan, M. M. A. & Ishfaq, M. (2021) Impact of Green Trust and Green Perceived Quality on Green Purchase Intentions: A Moderation Study. Environment, Development and Sustainability: A Multidisciplinary Approach to the Theory and Practice of Sustainable Development, 23 (9) September, pp. 13418–13435.

Werliin, R. & Kokholm, M. (2020) Insights 2020 - Device Usage [Online]. AudienceProject. Available from: <https://www.audienceproject.com/wp-content/uploads/audienceproject_study_device_usage_2020.pdf?x56703> [Accessed 18 December 2020].

White, H. & Carvalho, S. (2005) Combining the Quantitative and Qualitative Approaches to Poverty Measurement and Analysis. EconWPA, Development and Comp Systems, January.