DOCTORAL RESEARCH CONCEPT

TITLE OF PHD DISSERTATION:
Complexity Reduction and Operationalization of the GDPR:
Conceptualization of a User-Oriented Online Privacy Control System and Evaluation of its Effects on Organizational Trustworthiness

AUTHOR:
Kadir Ider

PHD SUPERVISORS:
Prof. Todor Ganchev, PhD
Prof. Svetlana Lesidrenska, PhD

REVIEWERS:
Prof. Siyka Demirova, PhD
Assoc. Prof. Kapka Manasieva, PhD

PHD PROGRAM:
Organization and Management of Production (Industry)
Dept. of Industrial Management

DATE:
28.02.2023

Table of Content

List of Figures

List of Tables

1. Introduction

The aim of this study is to develop a pragmatic, scalable, and cross-industry-applicable user-centric privacy control system with minimally disruptive organizational design properties. This research is informed by analytical research and a literature review of the solutions to the problem of online privacy control, both globally and in particular the European Union.
The outcome of the study is expected to provide trustworthy features and information requirements that must be integrated into the online privacy control system to earn the effective trust of individuals towards data processing organizations.

2. Analytical research and review of the global and regional solutions to the problem

2.1. Analytical research with a literature review

2.1.1. Topic Relevance – Societal Impact of Privacy

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). Particularly online shopping and banking are cohesive and associated with collecting and processing personal (and to some extent sensitive) data.
The rising number of personal devices and progressive digitization of services add additional verticals for personal data collection. The growing data access points require individuals to undergo a “privacy approval procedure” each time their data is collected. Although the GDPR requires the provision of policies and other privacy-related information prior to data collection, users do not perceive the communication as effective (Ider, 2020a, p.105).
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, in the context of Recital 23 GDPR. A subsequent non-compliance can result in fines of up to 20 million Euro or 4% of the preceding global annual turnover, whichever is higher, according to Art. 83 GDPR.
Nearly 2.5 years after introducing the GDPR, ⅔ of all German organizations struggle to meet full compliance (Dehmel & Kelber, 2020, p.2). 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).
Users tend to confirm the existence of a privacy policy but struggle to (1) effectively understand the content of the policy and (2) lose sight of the organizations to which personal data is disclosed. The results of a survey validate and reinforce this condition (Ider, 2020a, p.103).
According to the respondents, the communication of privacy is not satisfactory and therefore scores 3.85 out of 10 points for the integration of privacy modalities on average. Therefore, about 96% (Ider, 2020a, p.105) of users tend to read the privacy policy only marginally or not at all, whereby elementary data subject rights are already disregarded. Similar behavior is observed in external research results and thus substantiates self-collected data (Forsa Umfrage: Alles unter Kontrolle?!, 2018). The study further shows that half of the individuals experience a loss of data traceability, i.e., do not know the number of organizations that process their personal information at a given time.

1.1. Overview of Previous Research

1.1.1. State of Research

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) 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 3. 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.

1.1.2. Benchmarking of Models

A cross-industry-based assessment of contemporary privacy compliance-readiness of German organizations, labeled as “Current solutions”, is plotted in Figure 5 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". Particularly the user rights, which enable individuals to exercise their rights, are presented in detail in chapter 2.2.3. User definition of control. 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. Further elaboration is available in chapter 4. Conceptual Technical Infrastructure of the PPC.

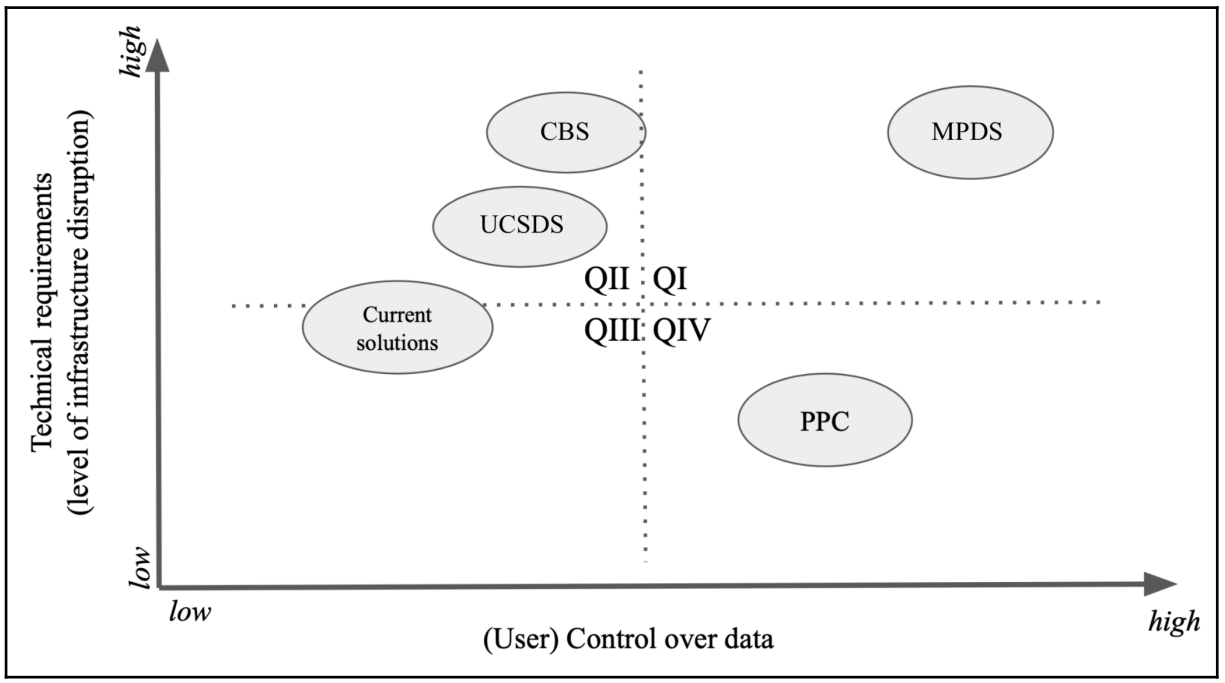

Figure 1: Adaptation Probability of Privacy System

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.

Figure 1 further 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, as pointed out in section 1.3.2 Technology as the Enabler and Obstacle. 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.

1.1.3. Conclusion of Paragraph

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.

2.2. Formulating the purpose of the doctorate

2.2.1. Problem Statement – Fuzzy Regulations and Lack of Practical Guidance

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, p.13).
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.
Table 1 reinforces the preceding findings by highlighting the fines clustered by nature of penalty:

Table 1: GDPR Penalties Aggregated Based on Regulatory Affiliation

Penalty Reason	GDPR Article	Penalty (in EUR)	Symbol
Non-compliance with general processing principles	5, 6, 7, 9	155,695,008.00	★
Non-compliance with data subjects rights	12, 13, 14, 15, 17, 21	50,217,941.00	◇
Insufficient compliance with controller and processor obligations	24, 25, 28, 31, 32, 35, 37	23,112,541.00	▲
Inadequate cooperation with data protection authorities	33, 58, 83	10,090.00	●

Almost 70% of all fines are attributable to non-compliance with general provisions and processing principles, 20% due to violation of data subject rights and 10% due to failure to comply with processing obligations. Despite its relatively small penalty amount, it is noticeable that inadequate cooperation with data protection authorities directly impacts the other infringement types.

The symbols presented in Table 1 are in correspondence with Figure 1. The Figure shows 477 penalties imposed between May 28th, 2018, and December 12th, 2020, clustered by penalty reason. It is noticeable that 96% (absolute: 458) of all penalties are less than 1 million Euro and amount on average to 1100 Euro. On the contrary, the major fines, 4% (absolute: 18), are above the threshold and amount on average to 12.7 million Euro. As of December 2020, over 99.8% of the total fine amount is represented by the major fines. At the time of research, it is still unresolved whether the penalties are firmly determined or yet to change as affected organizations may enter into appeal.

The density of data points alongside the time axis shows an increasing frequency of imposed penalties in recent periods. According to the Figure below, European data protection authorities have hardly issued any monetary penalties in the first six months after the GDPR came into force. Therefore, it is to be expected that the frequency will further increase, while most fines will level off at 1100 Euro on average. Although the number of imposed fines is at 477 and tends to rise, it is essential to point out that 22.24 million companies exist in the European Union, excluding the United Kingdom (Eurostat, 2020). Such organizations process personal information to some extent and are therefore subject to the GDPR. Effectively $2.15 \times 10{-}5$ (0.0000215)% of all European entities have been fined as of Dec. 12. 2020, conditional that all fines imposed are recorded.

The top five penalties (ordered by amount) have been imposed on Google, H&M, TIM Telecom Italy, British Airways and Marriott International for the cases of violation of data

subject rights, insufficient legal basis, and lack of technical and organizational information security measures.

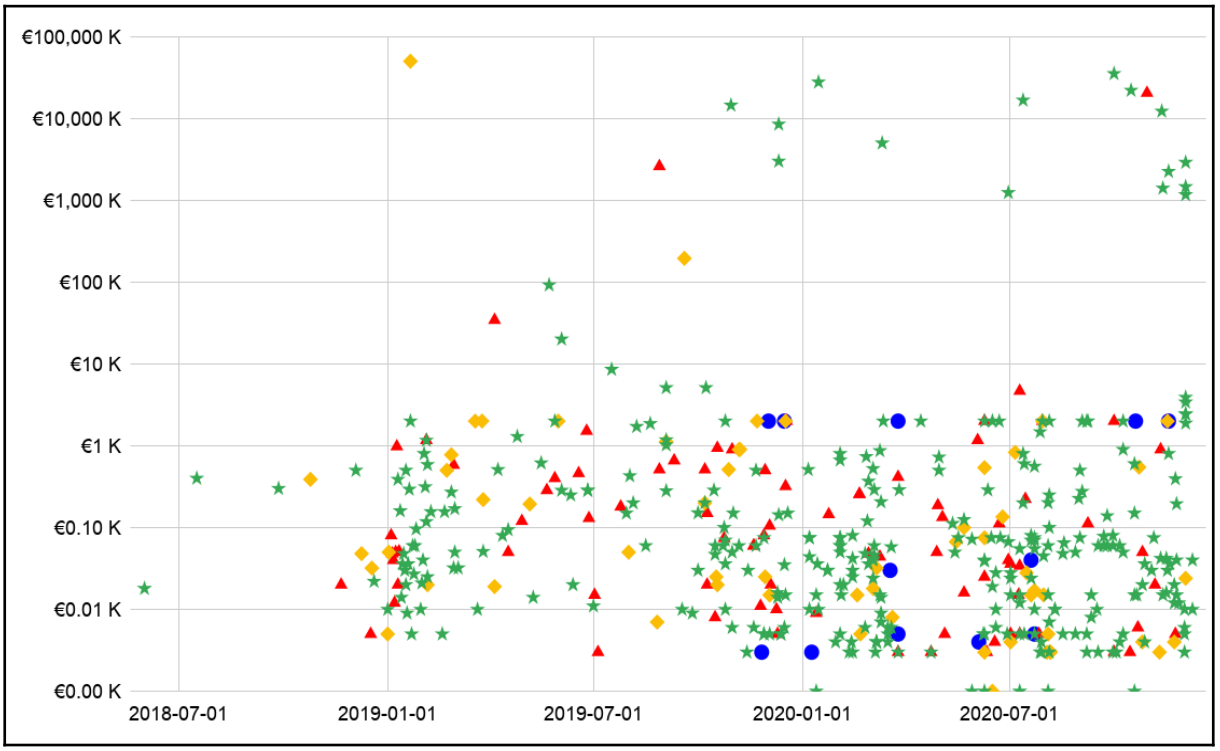

Figure 2: GDPR Penalties Plotted on the Time Axis and Infringement Class. Penalties are Presented on a Decimal Logarithm Scale (Ider, 2020b).[1]

A corresponding chart with the cumulative fines is presented below, in Figure 2. The blue line, resp. The area below shows the incremental growth of imposed fines within the European Union since the inception of the GDPR. The fine period extends to Dec. 12. 2020 and is identical with Figure 1. The red line represents an exponential trendline and reveals that the imposed fines increased accordingly over this period[2].

[1] Fines are stated in thousands of Euros (K).
[2] In appendix 4, a chart is made available, displaying the detailed information on GDPR penalties from 2018 up until 2022.

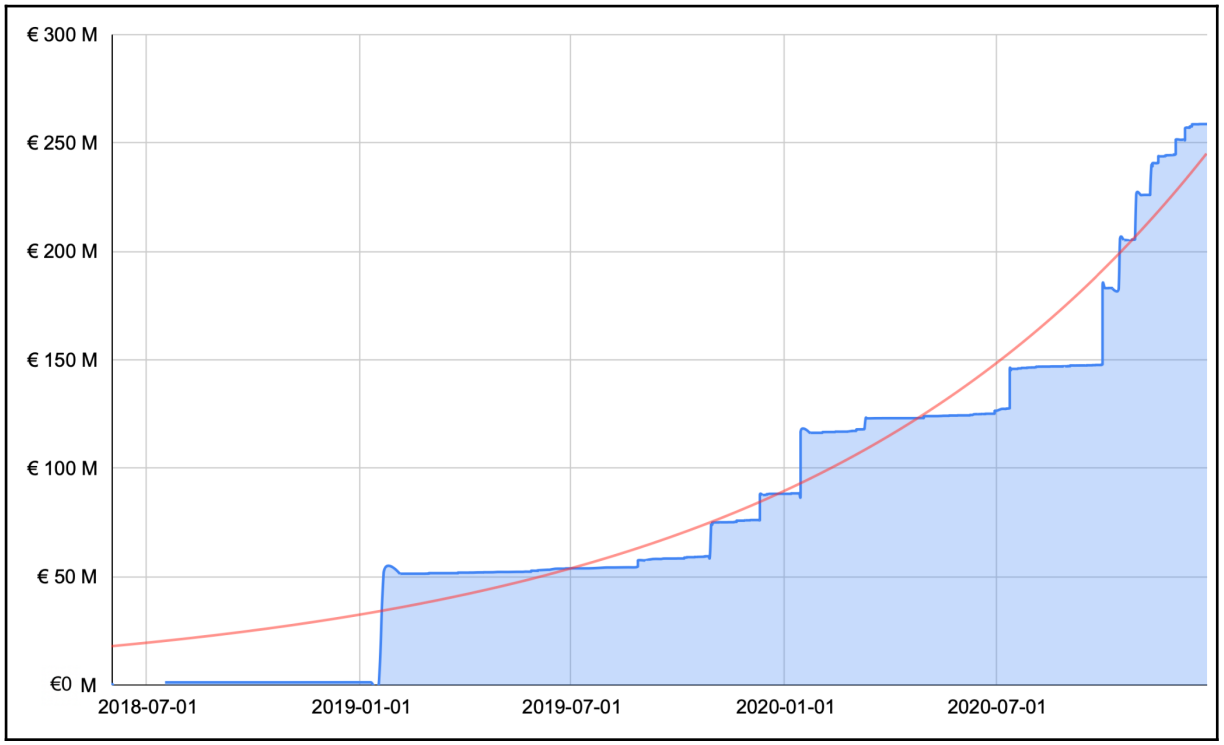

Figure 3: Cumulative GDPR Penalties Plotted on the Time Axis [3, 4]

2.2.2. Technology as the Enabler and Obstacle

The availability and communication of privacy modalities to individuals is an integral part of the GDPR. Especially in the digital engagement with subjects, e.g., via web presence or mobile apps, technology plays an essential part in privacy communication and ensures compliant processing throughout the entire data lifecycle.

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. This condition is further complicated by the scope and impenetrability of legal requirements (Faustino-Bauer & Ider, 2020, p.248). As such, organizations cannot effectively design user-oriented tools that allow individuals to oversee and control their personal data (Ider, 2020a, p.105). The consequences are immediately reflected in the imposed penalties displayed in Table 1 as well as Figure 1 and 2.

The foregoing analysis highlights the challenge to comply with the principles and lawfulness of data processing while maintaining an underlying secure technology landscape for meeting GDPR compliance throughout the entire data processing lifecycle. Both elements, principles and lawfulness requirements are further presented in section 4.1.2 Organizational Information System Requirements and Security Dimensions and concerning the security requirements in

[3] Fines are stated in million Euros (M).
[4] An extended plot of cumulative fines can be found in appendix 4.

3.2.2.2.3 Information System Control Measures. While technology remains a significant challenge for achieving GDPR compliance, it is parallelly the critical element for translating legal requirements into organizational processes for achieving adequate data protection and user-friendliness. This, in return, is a prerequisite to (a) become accountable for the obtained user information, (b) understand the effects of data processing technologies on data subjects and (c) implement effective privacy communication systems to ensure transparency towards individuals. The latter point is essential as it represents the interface between the data controller and the data subject, i.e., the data processing modalities are communicated at this stage, and individuals subsequently disclose data to organizations.

2.2.3. The Data Protection Compliance Dilemma

Based on the summary in the previous chapters, the major cornerstones of the data protection compliance dilemma are pointed out, i.e.,

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

2.3. Tasks to be solved to achieve this goal

2.3.1. Criteria Elements for Success, Quality and Effectiveness of Research

The development of a user-centric control system concept that is GDPR-compliant, pragmatic, scalable and cross-industry-applicable is in the scope of the research. Therefore, critical elements for a successful research outcome are:

- the identification and analysis of critical functional and technology features,
- the theoretical design of a privacy control framework as well as
- the evaluation of user control concerning privacy features and its effects on organizational trust.

The quality of the identified model features will be put together and assessed in the scope of a working model. Moreover, the identification of trustworthiness-creating elements will further enhance the quality of the privacy system. In the course of the dissertation, it is additionally discussed whether minimally invasive technology features determined in the research lead to higher adoption rates.

2.3.2. Research Objectives

The final research outcome shall provide private and public organizations with a feasible concept for a user-oriented online privacy control system. The final research outcome further lays down critical success elements, which organizations should consider when implementing the privacy control system.

2.3.3. Target Group: Beneficiaries of the Research

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.

2.3.3.1. Individuals

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. A thorough definition of the term individual is provided in chapter 2.1.2. “User”: Natural Person and Personal Data.

2.3.3.2. Public and Private Institutions

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[5].

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

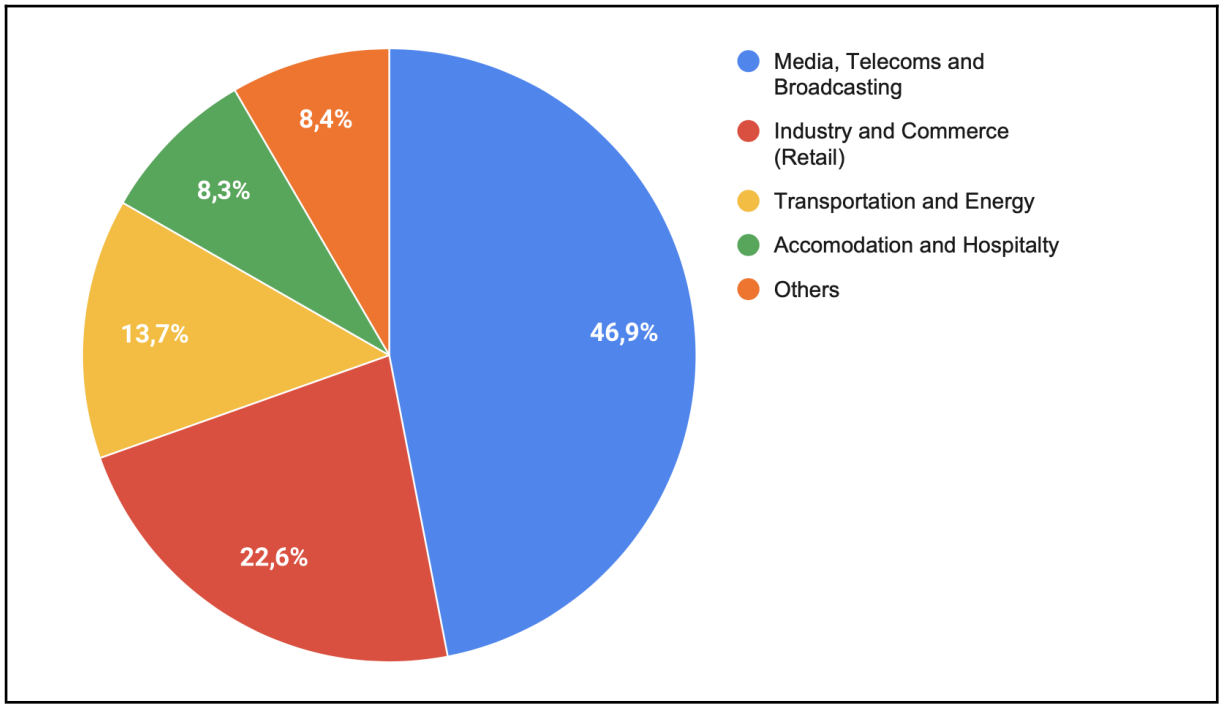

Figure 4: Proportions of Industries Affected by GDPR Fines (Ider, 2020b).

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.

2.3.4. Research Motivation

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 research goal is to provide the much-needed application oriented social innovation and demonstrate the expected social impact by purposefully developed GDPR tools and services.

2.3.5. Limitations & Assumptions

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). Thus, 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 participants will be offered to freely provide their email addresses, if they plan to participate in the raffle in the scope of the research[6]. The proportional number of users that will enter their data will further provide evidence and validation for the whole data set.

2.4. Conclusion

The introduction of the research topic identifies and defines the critical areas for developing a user-centric privacy control system. An increasing number of devices capable of data collection, loss of data traceability and individuals' lack of understanding need to be considered in further development. The challenges from an organizational perspective arise from the lack of practical guidance and implementation understanding of the GDPR. It has been identified that the GDPR lays down requirements but does not provide an end-to-end roadmap for achieving effective compliance. In addition, it is expected that the frequency and

[6] Survey participants can win online shopping vouchers.

number of fines are likely to increase faster than before. Moreover, organizations face a two-way challenge adapting existing infrastructures and parallelly operationalizing techno-legal requirements imposed by the GDPR. The two main interest groups (target groups) highlighted in the introduction include individuals and organizations as their counterpart. Both target groups are immediate beneficiaries of the expected improvements of user privacy control and GDPR compliance. Regulators will benefit from a centralized system by gaining a more comprehensive perspective on the needs and practices of both users and companies. Based on the preceding research findings, critical cornerstones for measuring the success and the limitations of the research are derived and specified. These key challenges and the need for effective compliance are at the core of developing a solution and will be addressed in the following chapters.

3. Theoretical formulation of the decision and tasks to achieve the goal

3.1. Organizational models

3.1.1. Introduction to Research Methodology and Tools

The research methodology involves the analysis and theoretical conceptualization of the Personal Privacy Cockpit (PPC). A qualitative semi-standardized survey will take place to collect user data regarding the feature importance of the privacy system and the assessment of the trustworthiness towards organizations. The data collection will be channeled via Qualtrics and Google Forms and communicated through various platforms (e.g., Workplace, LinkedIn, Twitter) to reach a representative set of participants.

3.1.2. Preliminary Study Results

A preliminary survey, available to all Delivery Hero SE (DHSE) affiliations and LinkedIn members globally, has been conducted with N = 100 respondents[7] to identify the user requirements regarding privacy control and consequently narrow down the focus area (Ider, 2020a, p.104). The respective platforms have been selected due to the ease of user data accessibility and limitations to resources, time, and budget. The survey questions are designed to capture self-reported opinions (attitudes) from a user perspective and to some extent detect behavioral insights and further minimize any work-related association (Ider, 2020a).
The survey incorporates demographic data, opinions on the effectiveness of organizational privacy solutions and the option to select between two control systems designed to promote effective privacy control. Both the responses of DHSE employees and LinkedIn members have been analyzed and compared in an isolated manner. The results show a similar response pattern in both survey scores. A limitation to the survey is the level of education of all participants, as they hold a degree of higher education (Ider, 2020a). This limitation is partially offset in the main research survey through the collection of data from individuals irrespective of their degrees, but rather through the coverage of a wider range of qualification levels and across various industries.
However, despite the utilized distribution channels, this limitation may not be fully compensated. Key information concerning the demographic data from preliminary study (Ider, 2020a):

- demographic (incl. EU and Non-EU): 67% of the observations originate from the EU and 33% outside the Union, in total 32 countries,

[7] N = 100 at the time of the publication of "Effective Privacy Management Concepts: Increasing Privacy Control by Reducing Complexity". N = 151 as of January 3. 2021, whereas no drastic deviation of data is visible.

- demographic (only EU): 67% of the EU-based observations originating from Germany; consequently, average measures are applied to level-off effects of such large groups,
- gender distribution: approximately 50% men, 45% women and 5% either diverse or preferred not to give information on their gender,
- age range: 67% of the observations are in the age range between 26 to 35,
- 1/3 of all participants work in tech-related jobs; however, an isolated data analysis of this group shows no significant deviation from the overall results,
- preferences regarding privacy control system: 92% of respondents prefer the PPC over the SPL solution.

A short description of both systems, PPC and SPL is provided below:

- Standardized Privacy Layout (SPL)

  A standard privacy framework proposes the same privacy layout, i.e., using the exact wording, icons, and layout structure to ease the navigation in the privacy section of any online service provider that collects personal data. The website owners would still be responsible for accurately specifying the data they collect about individuals and maintaining GDPR compliance.

- Personal Privacy Cockpit (PPC)

  This is a user-centric management platform for personal information management. The PPC provides a dashboard that is connected to various organizations, which obtain and process personal data. It shows where and how personal data is used online. Once an account is set up, users can use this for any online activities, e.g., signing up, shopping, but also monitoring purposes. The PPC will notify users, if changes are made in the privacy policies of online service providers or if personal data has been compromised.

3.1.3. User Behavior Towards Personal Data and Technology Benefits Trade off

The research findings of Lyons, Stokes, Eschleman, Alarcon and Barelka (2011) highlight that people with a higher level of IT suspicion engage in a more extensive search for information, whereas the level of trust can coexist independent of suspicion. These results are validated by a survey conducted in the scope of a preliminary study for this doctoral thesis (Ider, 2020b, p.106). 5% (n = 8) of all respondents claim to spend more time carefully reading privacy modalities offered on websites of organizations. On average, this group is less willing to trade

off their personal data for the technology benefits, either due to higher levels of distrust or IT suspicion, or both factors together. In contrast, nearly 95% (n = 143) of all respondents, either marginally or do not at all read the privacy modalities before sharing their personal data. On average, the same group is somewhat willing to trade off their information for the benefits of technology, as shown in Figure 6. However, this is neither evidence that higher levels of suspicion lead to a decreased trade off willingness, it is the limited level of trust, or altogether.

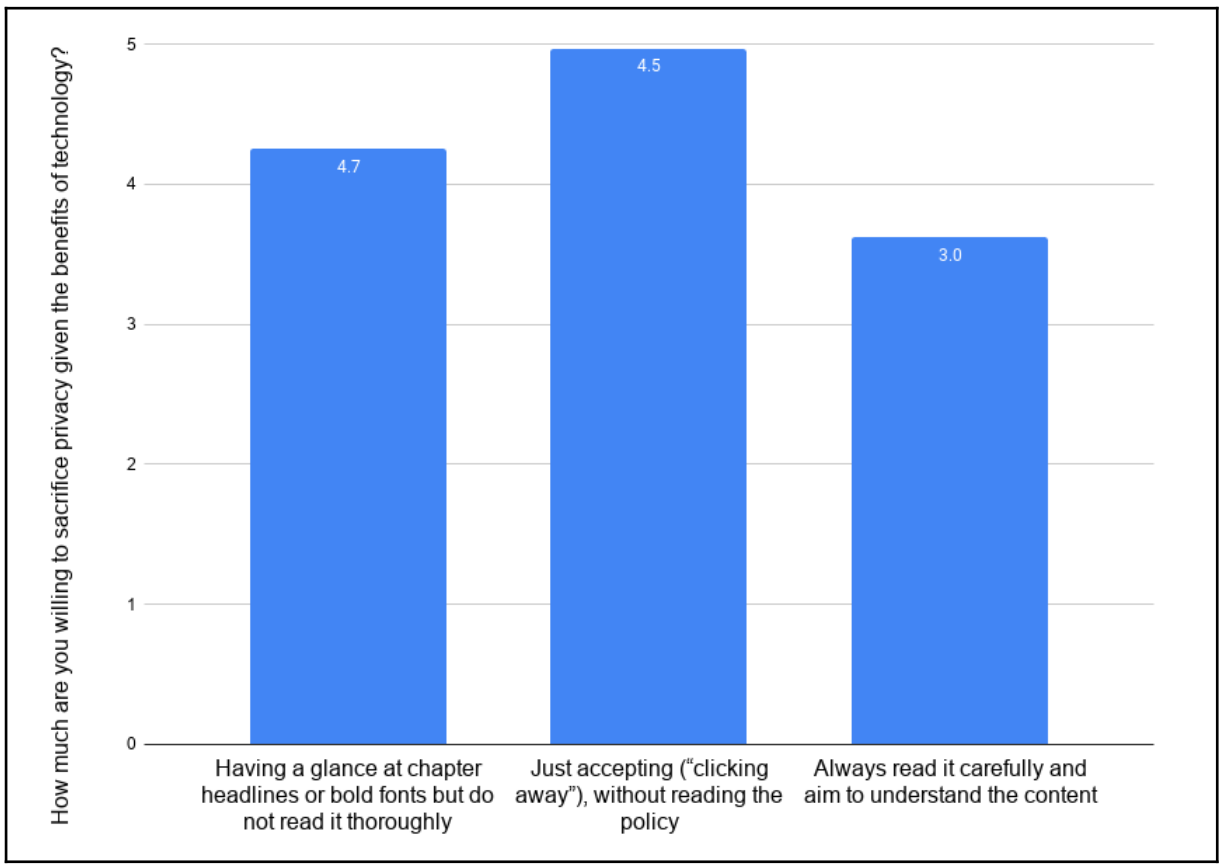

Figure 5: Willingness to Trade off Personal Data for Technological Benefits

This evaluation reveals new findings and, concurrently, raises new questions regarding the trustworthiness of privacy control systems, specifically, the mutual interdependence of trustworthiness and IT suspicion, which will be analyzed during a survey.

3.1.4. Working Hypothesis

The hypothesis is derived from the findings of the preliminary survey and the gaps identified in the literature review. It concludes that shifting some control to the user is more beneficial than entirely leaving the user responsible for managing their personal data (Ider, 2020a). Shifting sole control of data to the user does not accelerate user adoption of new frameworks, due to increased complexity of the user interface and experience (UI/UX) as well as lack of

understanding of the GDPR. Therefore, the user will be able to use a limited set of functions and features identified in the scope of the surveys. The hypothesis will be tested for its robustness through a qualitative research approach.

3.1.5. High-Level Research Design and Data Analysis Structure

This chapter provides a structural understanding of the subsequent research structure, reflected by the four elements (provided below) and relevant stakeholders. The research design approach partially follows the structure of the NIST risk management framework. It allows addressing the various organizational requirements related to the design, development, implementation, and operation of such a framework (Joint Task Force Transformation Initiative, 2013, p.8). The following elements have been and include:

Element 1. Identification and Categorization of Input Parameters

The input parameters refer (1) on an aggregated level to the affected parties (Who is involved from an organizational perspective?), including individuals, organizations and (2) on a granular level to the specification of elements (What are the relevant features?), such as identification of data subject rights, technical and organizational security features, adequate documentation and communication of policies and procedures, which must be evaluated in detail.
Understanding each element and the interdependency of the affected parties across the identified input parameters is the basis to measure their weighted impact on the online user control system and ultimately on the level of effectiveness of the tool. Furthermore, the weighting facilitates the classification of the criticality levels of individual parameters. The ultimate beneficiaries are the individuals and organizations and their mutual interactions.

Element 2. Selection and Assessment of Control Elements

The control elements that users and/or organizations engage with, which have been identified as critical, will be in the scope of the detailed assessment. The survey data will be primarily used to measure the effectiveness of the system features from a user perspective. Furthermore, the identified trust-building elements will be assessed as well.

Element 3. Implementation of Final Findings

This process step involves implementing identified system features in a manner that facilitates an effective control solution for individuals and allows the operationalization of the GDPR. The implementation is limited to a descriptive presentation of the end-to-end view of the

system. The user interface and functionalities as well as the comprehension of the underlying technology and its associated security features are the goals of this process step.

Element 4. Revision and Discussion

Once the final structure is built, quality assurance in the scope of a retrospective discussion will provide a critical evaluation of the research and development phase as well as the final system.

3.1.6. Interim Summary of Survey Design and Structure

The mixed-method approach, which involves collecting qualitative and quantitative data, aims to collect and assess data to measure the effectiveness of identified control elements as well as evaluate the trustworthiness creating features and interdependencies among such elements. Consequently, this integrated approach (White & Carvalho, 2005, p. 16) eliminates the need to conduct two separate surveys but combines the two stages in one. While the quantitative dimensions deliver insights on the distribution of a particular topic, the qualitative dimension provides deeper insights into why users behave that way. An additional data quality element is the quantification and precise reasoning provided by the same individuals.

3.2. Legal Models

3.2.1. Terms & Definitions

3.2.1.1. Relevant Definitions of the GDPR

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.

3.2.1.2. Territorial Applicability and Boundaries

The territorial scope of the GDPR is set out in Art. 3 and addresses the jurisdictional application of the regulation. The article differentiates between the following three common scenarios:

- if a controller or processor is established in the EU, irrespective if the affected individuals are EU residents or not,
- if a controller or processor is not established in the EU, but processes personal data of EU residents[8], e.g., providing goods or services to such individuals,

[8] Attention: resident is not synonymous with citizen. It is possible to be a non-EU citizen but an EU resident.

- if a controller or processor is not established in the EU, but processes personal data of EU residents in the scope of monitoring the behavior of individuals.

Subsequently, the GDPR does not apply to other jurisdictions outside the EU, i.e., organizations that do not process personal information of EU residents. In addition, EU residents who reside or spend time abroad and use products or services in the respective non-EU country are not entitled to data protection under EU law. As further elaborated in subsequent paragraphs, the GDPR does not apply to personal data of deceased residents of the EU.
Furthermore, the GDPR does not apply to data that has been anonymized, i.e., where the chance of re-identification of individuals is either not possible or only possible with significant resources and efforts, according to Recital 26 GDPR.
Nevertheless, a broader range of application of the proposed solution is certainly not ruled out. The applicability of the system is therefore not limited to affected organizations but can also find its applicability in other countries with similarly established data protection regulations, such as, but not limited to, Singapore (Ministry of Communications and Information, 2014), Hong Kong (Office of the Privacy Commissioner for Personal Data, 1995) or Japan (Personal Information Protection Commission, 2016).

3.2.1.3. The "User": Natural Person and Personal Data

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.

Besides the general definition of personal information, the GDPR further specifies special categories of personal data in Art. 9 (1), which include:

> [...] personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

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):

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

It is capturing all personal data that an organization process contributes to an effective user privacy control. Therefore, it is essential to consider such non-obvious identifiers, respectively, to provide guidelines for determining any data that potentially lead to the identification of a person. Recital 27 of the GDPR limits the applicability of the regulation, as the "regulation does not apply to the personal data of deceased persons. [However,] Member States may provide for rules regarding the processing of personal data of deceased persons."
Consequently, while the scope of GDPR does not cover the personal information of deceased individuals, the protection of such data may vary across the European States.

3.2.1.4. Processing: Definition, Opportunities and Restriction

The GDPR defines processing in Art. 4 (2) as follows:

> 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Thus, a generalization can be drawn from the definition, i.e., processing includes any activity from the first recording up until the destruction of personal data. Therefore, personal data must be included in the online privacy control system for at least if data is being processed.

3.2.1.5. Principles of Data Processing

The General Data Protection Regulation lays down data processing principles in Art. 5 - Art. 11. The two primary definitions are the purpose (Art. 5) and lawfulness of processing (Art. 6). They are considered particularly important as they specify fundamental elements for compliant processing and represent the most frequent source of violation leading to 70% of all imposed fines. Therefore, these articles are subject to a detailed definition.

The principles relating to the processing of personal data in Art. 5 of the GDPR are summarized in the table below. They are essential for the further analysis conducted in chapter 4.1.2 Organizational Information System Requirements and Security Dimensions:

Table 2: GDPR Principles and their Implications

Art. 5 GDPR Principles	Meaning
Lawfulness, Fairness and Transparency	● Lawfulness: processing of personal data may only take place upon a legal basis ● Fairness: scope of processing must be limited to the extent that an individual can reasonably expect ● Transparency: the level of honesty and openness towards the individual concerning the processing of their data
Purpose Limitation	Data processing must meet the following criteria: ● Specificity and Legitimacy: A specific purpose must be defined ahead of the processing, as data retention, i.e., collection for a non-specified purpose, is not allowed. Moreover, the specified purpose must not include multiple or different purposes, unless they are compatible with the original purpose.
Data Minimization	Data processing must meet the following criteria: ● Adequacy: the data must be appropriate, necessary, relevant, and limited to the extent for fulfilling the purpose
Accuracy	● Data integrity must be protected throughout the entire data lifecycle. Consequently, incorrect data must be rectified without undue delay and kept up to date.
Storage Limitation	● Data must only be stored (any storage type, e.g., physically, or digitally) for the period for fulfilling the purpose and, thus, must be deleted upon completion of the purpose. ● Identification of individuals shall only occur where it is necessary, i.e., personal data shall be masked, where identification is not necessary.
Integrity and Confidentiality	● Art. 5 (1) lit. F protection of data “against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures” ● see 3.2.2.2.3 Information System Control Measures for further specification
Accountability	● the ability to demonstrate above mentioned obligations throughout the entire data processing lifecycle ● Liability: bear the consequences of misconduct and subsequent monetary fines and reputational damages

The lawfulness of processing is defined in Art. 6 GDPR and can be followed by the obligation that arises in Art. 5 (1) lit. a GDPR. The lawfulness provides a juridical ground for the processing. There are six bases, which are further defined in 4.1.2 Organizational Information

System Requirements and Security Dimensions. Generally, irrespective of the underlying lawful basis, the organization must consistently prove its compliance with the GDPR.

3.2.1.6. Profiling

The General Data Protection Regulation defines in Art. 4 (4) that:

> 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

Art. 22 GDPR further specifies that:

> [the] data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

In consideration of both articles, it is relevant to provide a section in the privacy control system that declares the nature and scope of the profiling, if such activity is carried out or is expected to be carried out.

3.2.1.7. The Organization: Controller Types, Processors, and their Obligations

The term "organization" in the scope of this research refers to any institution that processes personal data. 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, irrespective if it is a natural or legal person or a public authority. Moreover, the controller is the entity that enters into a contract or has a direct relationship with individuals. As the controller is in such a privileged position and realizes commercial benefits from the data processing, it is – in consequence of that – the liable party for violations against the GDPR.

There are two additional controller constructs, i.e., the joint controller and the multi-controller (the latter case also referred to as the controller-to-controller relationship). Article 26 (1) GDPR defines "where two or more controllers jointly determine the purposes and means of processing, [...] they shall be joint controllers". In circumstances where controllers directly or indirectly obtain personal information from individuals, there is an obligation to communicate that to the affected person by the respective controller, according to Art. 13 and 14 GDPR.

However, besides a common purpose and interest in data processing, a joint controller is different from a multi-controller, as in latter case controllers (1) do not jointly design and (2)

maintain the underlying processing systems but (3) mutually exchange personal information across each other's systems. In such a scenario, each controller (4) keeps complete power over the system. Consequently, the (5) IT management requirements vary for the respective controller. Those five features may indicate a multi-controller over a joint controller relationship. Such fine differentiation is relevant to consider to compliantly obtain and process personal data and regulate the responsibilities among organizations and the obligations towards individuals. A processor is considered to exist when – according to Art. 28 GDPR – the "processing is to be carried out on behalf of a controller". Thus, two conclusions can be drawn: First, the processor has neither the power to determine the purpose and means of processing nor the direct privilege to realize commercial benefits from the data. Second, it is the controllers' obligation to only contract processors that provide "sufficient guarantees to implement appropriate technical and organizational measures". A violation of the GDPR caused by the processor would hold the controller accountable and liable for the damages to individuals and the processor. As processors must primarily meet the requirements set by the controller, their focus lies in guaranteeing adequate security measures, which essentially reflects the processor-controller relationship. Whether single, joint or multi, to sum up the various types, the controller has the primary obligation to ensure compliant processing, as he is in the immediate relationship with the natural person. Consequently, the main initiative, to implement the privacy control system, would be the controller's responsibility. Effective compliance could easily be met by connecting and communicating the privacy modalities to the individual via the control system.

3.2.1.8. International Data Transfers

Transfers of personal data to third countries or international organizations are defined in Art. 44 - Art. 50 GDPR. For effective communication of privacy modalities to individuals, the most important elements include (1) the transparency concerning the transfer of personal data to third countries during the processing, (2) the legal basis for the international transfer of data as well as (3) the adherence to the condition that the recipient in the third country meets the minimum requirements for technical and organizational measures.

3.2.1.9. Data Protection by Design and Default

Data protection by design and default, also known as privacy by design and default, already existed before the GDPR. However, since it came into effect, the respective obligation has become a law and thus must be integrated throughout the entire data processing. In this context data protection will be used synonymously with privacy. The duties of the controllers are set in Art. 25 (1) and (2), whereas Art. 25 (1) outlines the requirements for privacy by design:

> Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this regulation and protect the rights of data subjects.

The article already requires considering privacy in the development phase of a product, service, or system by identifying and implementing state-of-the-art security measures, protecting user rights. According to the European Data Protection Board (EDPB), such services could range from the mere definition of a policy or internal guideline to developing a new service for customers (2020, pp.15-17). The implication for the privacy control system that arises from the regulation is the requirement to design it already data protection friendly. This will be incorporated into the various levels of development.

Art. 25 (2) specifies the obligations towards controllers to include privacy by default:

> The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

According to the article, the developed product, system, or service should – by default – obtain and process data to the minimum level, which is required to fulfill a purpose. Moreover, the user shall have the ability to actively “intervene”, i.e., control the level of personal information that is disclosed. It is essential to notice that even users must allow a certain amount of their data to be processed to receive the respective goods or services from an organization. The challenge for the proposed privacy control system is to embed technical features that extract relevant information from any organizational system and reflect it accurately to meet privacy by design requirements and in a broader scope to adhere with the GDPR.
The preceding evaluation highlights additional feature opportunities and limitations for the privacy control system. Consequently, a balancing of (additional) features with the associated extra effort for implementation will occur. This step is elementary to ensure that the control system provides an adequate level of private information while limiting the implementation complexity for organizations. Ultimately, privacy by design and default provides key data protection instruments (Voigt & Bussche, 2017, p.62) for organizations to meet their obligations.

However, this also means that the privacy control system is limited to the interface management between users and organizations, while it does not impact the compliance quality of organizational systems internally.

3.2.1.10. Impact of GDPR Definitions on Framework Development

The GDPR definitions highlight essential features that the privacy control system should incorporate, including the basic elements that facilitate transparent intelligibility of the data and the underlying processing. Key features that will be included in designated sections are information regarding the controller(s) and processors, territorial applicability, principles of data processing that the organization follows, the purposes for which they collect data, categories of personal information, the respective lawful basis, profiling undertakings and international data transfer specifications. Additionally, a discussion will be devoted to the technical complexity of the control system and how to limit it in order to reduce the cost of the system integration and improve its value proposition. Nevertheless, due to legal requirements, system security and control requirements must also be met by the privacy control system and will therefore be considered in the context of the dissertation.

3.2.2. Definition of Control

In the following subchapters the term control will be 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. 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 fundament from which technical and user control elements are derived.
As discussed in the foregoing analysis, the 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.

3.2.2.1. Legal Definition of User Control

While the subsequent technical and psychological definitions are means to meet and measure the level of user control, the regulatory analysis builds the foundation and achieves legal, especially GDPR compliance. The first compliance obligation, the user rights, are specified in Art. 12 – 23, are the basis for the definition of the user control requirements and will be defined (see table 3).
Technical requirements in accordance with Art. 32 GDPR are covered by the 14 security requirements of section 64 of the German Federal Data Protection Act, see 3.2.2.2.3.

Information System Control Measures. Since technological requirements prove to be of great complexity it must be consistently maintained to achieve user control.

Table 3: User Control Elements According to Art. 12 – 23 GDPR

Article	Specification
12	transparent information, communication, and modalities for the exercise of the rights of the data subject
13	information to be provided where personal data are collected from the data subject
14	information to be provided where personal data have not been obtained from the data subject
15	data subjects right to access personal data
16	data subjects right for rectification of personal data
17	data subjects right for erasure (‘right to be forgotten’)
18	data subjects right to restriction of processing
19	notification obligation regarding rectification or erasure of personal data or restriction of processing
20	data subjects right to data portability
21	data subjects right to object processing
22	data subjects right to object automated individual decision-making, including profiling
23	restrictions that Union Member State laws can impose on the processing of personal data

3.2.2.2. Technological Definition

The technological definition specifies the second dimension of control. It provides the physical means to meet the control requirements identified in the legal context. Ultimately, technological control refers to the features that an information processing system provides to (1) manage data and maintain underlying systems and (2) allow ownership and transparency of data in the user context. Technological control is characterized by the National Institute of Standards and Technology (NIST) through multiple attributes, which aim at ensuring control on an organizational, operational (business process) and information system level (Joint Task Force Transformation Initiative, 2013).
Any measure implemented at the operational level is immediately applicable at the organizational level and vice versa.

Therefore, organizational, and operational control are both covered by the configuration control (2.2.2.1), the audit review (2.2.2.2) and the information system control (2.2.2.3), which define the measures (features) as specified below:

3.2.2.2.1. Configuration Control

Configuration control refers to the traceability and transparency of changes made to hard- and software (Kissel, 2013). It should protect affected systems from undesirable alteration throughout the entire system lifecycle.

3.2.2.2.2. Audit Review

The system audit function adds a layer for post-data-processing control, i.e., the technical ability to retrospectively review and evaluate the affected information system (Kissel, 2013). It provides a key feature to maintain adequate functionalities to ensure data integrity and identify and mitigate potential system security flaws.
While it is not feasible to provide this feature to users, organizations should aim to enable audit review functionalities. This comes at a higher cost for organizations in the short run, but may be cost saving in the long run, due to improved services and increased compliance (Ruud, n.d., p.78).

3.2.2.2.3. Information System Control Measures

The criticality of a system will impact the level of (additional) security control measures that need to be in place (Kissel, 2013). The NIST Tier-3 system approach categorizes systems upon their impact on the security objectives: confidentiality, integrity, and availability, also referred to as the CIA triad (National Institute of Standards and Technology, 2006).

As such, the security category of a system is considered high, as systems that process personal data will have a potentially high impact level and therefore must have to comply with the CIA triad.[9] The respective security functionalities will be derived from the German Federal Data Protection Act, which specifies 14 security requirements in section 64 BDSG, which have an immediate effect on the level of system control (for users and organizations), particularly for automated processing systems (Federal Ministry of Justice and Consumer Protection, 2017):

[9] A system that would only require one of the CIA elements would be considered as a low impact system. A system that would require two of the three elements would be considered as a moderate impact system and require all three elements considered as a high impact system.

- equipment access control
- data media control
- storage control
- user control
- data access control
- communication control
- input control
- recovery
- reliability
- integrity
- processing control
- availability control
- separability

The identified technological elements are feature specifications for both the user privacy control system and the data processing organizations, as shown in process step (2) and (3) in Figure 3. These specifications are used to ensure the security of all data-processing systems. While these control elements ensure technical and organizational security (internal control), they also serve to understand the internal data flows. As the workflow below suggests, the basic understanding of data flows and data security must be met to provide practical tools for users to exercise (external) control over some aspects of the data processing organization (1) through the privacy control system (4):

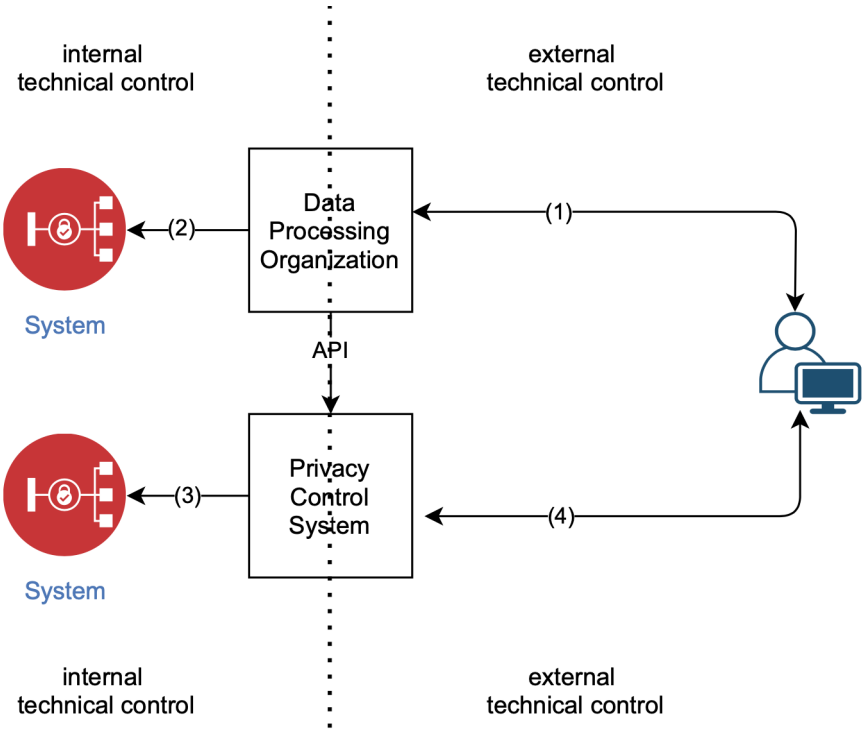

Figure 6: Proposed Technology Control Dimensions

In this workflow users are enabled to exercise control over their data (external technical control). Thus, it can be summarized that although technological control has different dimensions that need to be covered, the only way for a user to exercise control over his or her personal data is through tools or systems, represented by the dotted line that separates internal from external technical control. In particular, the assessment of control will be limited to the area between the user and the data processing organization, see workflow (1).
Despite the privacy control interface being the platform in which to exercise control, actual control always results from direct interaction between a user and an organization and is dependent on organizational capabilities to accommodate user needs. In part, users will be able to exercise their rights over the user privacy control system (4). This is further elaborated in 4.6.3 Technical Architecture, Element 2. User Interface.

3.2.2.3. Psychological Definition

This definition focuses on the intangible aspects of user control. In psychology there is a differentiation between various attributes and levels of control. A comparison of the definitions in major dictionaries, including the American Psychology Association (APA) Dictionary of Psychology and the Oxford Dictionary of Psychology, will be presented below to highlight the different elements. The psychological definition also encompasses the emotional assessment, which is considered a psychological state.
According to APA Dictionary of Psychology, control is defined as (VandenBos, 2015, p.247):

1. [The] authority, power, or influence over events, behaviors, situations, or people.
2. The regulation of all extraneous conditions and variables in an experiment so that any change in the dependent variable can be attributed solely to manipulation of the independent variable and not to any other factors.

Those key attributes will measure the psychological level of control over personal information via the online privacy control system. The measurement ranges from very positive to very negative emotional experience (Skinner, 2013). The Oxford dictionary (Colman, 2003, p.177) does not define the term control, but specifies the element of controlled processing, which provides a relevant dimension for the understanding of the term control in the scope of data processing and data processing systems:

> Any form of information processing requiring conscious attention or control, as in the performance of a novel or difficult task. Compared to automatic processing, controlled processing is generally much slower, requires more effort, […] and does not normally involve parallel processing of information from more than one sensory channel, but it can be developed faster and with less practice than automatic processing, often in a few trials, and it leaves the learner with greater control of the behavior.

The Oxford definition points out an important element, i.e., the differentiation between controlled and automated processing tasks. While controlled processing requires a higher degree of manual (i.e., human) interaction, automated processing does not require manual intervention. Consequently, the interface where manual control and automation engages will be further assessed in the scope of the research. The evaluation shall identify the degree of human control, i.e., to (1) which extend human intervention is possible and simultaneously (2) define the interaction and mutual effects of manual and automated processing.
While the development of the privacy control system is the central focus of the study, the results will also provide evidence on (1) its effectiveness and (2) its impact level on corporate privacy communication.

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

In social learning theory trust 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).[10] 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.
Approaching the definition of trustworthiness from an information technology perspective, i.e., according to the NIST Information Security Terms, the definition of trustworthiness from a user perspective is (Kissel, 2013, p.205):

> The attribute of a person or organization that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities.

[10] 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.

Whereas the definition of a trustworthy information system is (Joint Task Force Transformation Initiative, 2013, Appendix B p.25):

> The degree to which an information system (including the information technology components that are used to build the system) can be expected to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the system across the full range of threats. A trustworthy information system is a system that is believed to be capable of operating within defined levels of risk despite the environmental disruptions, human errors, structural failures, and purposeful attacks that are expected to occur in its environment of operation.

According to a study conducted by researchers (Lyons et al., 2011, p.224), trust and distrust are independent of general IT suspicion. Following Lewicki, McAllister, and Bies definition (1998, cited in Lyons et al., 2011, p.220), within this research framework, it is assumed that both the trust and distrust represent some degree of certainty (or uncertainty) in either a positive (i.e., trusting) or negative context (i.e., distrusting).
Lyons research approach goes further and identifies a third element, which is the level of suspicion towards IT systems. The research concludes that the level of suspicion correlates positively with greater engagement in information search, proportionally to the individuals with less suspicion.
IT suspicion will not be limited to either hard- or software but is assumed to include all underlying systems, logics and algorithms that are designed to process data. This includes a multi-layered perspective; thus, multiple technologies may be used parallelly in the processing throughout the entire data lifecycle. This conclusion poses three crucial questions about the multidimensional construct of trustworthiness, which are:

- Does a change in users' perception of data control influence the level of trustworthiness?
- How does user suspicion towards IT systems affect trustworthiness considering the age and experience of individuals?
- Will conciseness, transparency, intelligibility, ease of information access and the used language[11] in the privacy control system improve trustworthiness and decrease suspicion? Does this lead to a better understanding of the technologies that companies use to process data?

Following the findings of the various authors referenced in this research (e.g., Rotter 1980, Gul 1983, Andreoni & Miller 2002, Lyons et al. 2011), the time and effort that a user devotes to the privacy control system for information search should be more significant among

[11] within the meaning of Art. 12 GDPR

individuals with a higher level of suspicion among the younger and less experienced age groups than among those with inherently lower levels of suspicion among the older more experienced age groups. Therefore, the suspicion should decrease with the development of easily accessible information in the underlying IT systems used for data processing purposes. In order to examine this more closely, trustworthiness is analyzed from three perspectives:

1. trustworthiness of an organization from a user perspective concerning personal data processing,
2. trustworthiness of the underlying information processing systems,
3. level of suspicion towards IT systems and associated efforts for information search.

Hence, the envisaged method considers (1) the trustworthiness of an organization, with regards to personal data processing and from an individual perspective, as well as (2) trust-building components of underlying information processing systems.
Considering the aforementioned definitions of trust and trustworthiness, the trustworthiness-building features will assess the psychological, technical, and legal requirements concerning the processing of personal data, split into data, process and system.
Subsequently, trustworthiness features are derived from the respective disciplines. Based on the foregoing assessment, trustworthiness can be achieved or enhanced by the following factors documented in the table below:

Table 4: Trustworthiness-Building Key Measurement Indicators

		Organization		
		Data	**Processes**	**IT systems**
Control	**Psychological**	psychological control over data	psychological control over processes	psychological control over systems
	Legal	legal control over data	legal control over processes	legal control over systems
	Technological	technological control over data	technological control over processes	technological control over systems

A further concretization of key measurement indicators stated above takes place in the corresponding table below. Each indicator is mapped to one or more metrics that are specified in the survey. This allows a direct linkage of the data gathered from the conducted survey and indicators stated in table 4, resp. complementary table 5. Table 5 is further underpinned through a color scheme. 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.

Table 5: Concretization of Trustworthiness-Building Factors

		Organization		
		Data	**Processes**	**IT systems**
Control	**Psycho-logical**	- sharing of different personal data categories (non-sensitive and sensitive information) - inherent level of trust of organizations with respect to sharing personal data - links to fan page	- time spent reading/understanding privacy modalities - conciseness, transparency, intelligibility, ease of access to information of processing activities	- system feature controllability - access to technical and organizational security measures - degree of system functionality personalization
	Legal	- confidence of exercising user rights	- conciseness, transparency, intelligibility of privacy information	- certification and verification mechanisms for lowering risk perception and improving compliance
	Techno-logical	- reliability of data processing technology - confidentiality - integrity	- security of processing (Art. 32 GDPR) - (14 security requirements (section 64 BDSG))	- credibility - availability of data - reliability of a system

Legend: User-, Organizational-, Mutual Influence on trustworthiness

Lastly, an adequate level of trustworthiness should be achievable with ease of information access and the detailed level of available information, while the latter case shall minimize the distrust of individuals. This aspect of trustworthiness and its association to user engagements with online privacy solutions will be further elaborated in section 5.1 Preliminary Study Results. Although control over data may be achieved without the trustworthiness factor and vice-versa, it is worth emphasizing that this research looks at the common features and variables.

The identification of factors influencing both control and trustworthiness further establishes determinants that create efficient synergies, which leads to the faster achievement of the objectives of this research undertaking, i.e., for the conceptualization of the online privacy control system for users.

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.

3.3. Technical Models

3.3.1. Conceptual Technical Infrastructure of the PPC

3.3.1.1. Privacy Control via Personal Privacy Cockpit

The Personal Privacy Cockpit (PPC), also referred to as an online privacy control system or control system in the scope of this research, provides a central platform, where users manage their personal information. The PPC provides a dashboard displaying where and how personal data is used online.
Once a profile is set up, the user can use this for any online activities, e.g., signing up, shopping and monitoring where personal information is used, if changes have been made in the privacy policies of online service providers and if data has been compromised. This system shall improve the user's abilities to identify organizations processing their data, while also improving transparency and accountability obligations of organizations. A conceptualized version of the PPC mock-up web page is available here[12].

3.3.1.2. Organizational Information System Requirements and Security Dimensions

In the following, the designated system requirements and security elements considered in the scope of this dissertation will be discussed.

In its guideline "Security and Privacy Controls for Federal Information Systems and Organizations" (Joint Task Force Transformation Initiative, 2013, p.1) the NIST defines that the safeguarding of individuals requires the protection of data processing systems. Such systems must:

1. protect the confidentiality, integrity and availability of information that is processed, stored, and transmitted by those systems/organizations and
2. satisfy a set of defined security requirements.

It is essential to consider the security control requirements, as they substantially enhance privacy control from an organizational security perspective. To prove accountability, these requirements must be consistently fulfilled in an effective manner throughout the processing lifecycle. The NIST lays down the basis for privacy control, i.e., to protect and ensure the proper handling of personally identifiable information (PII).

[12] Link for manual entry: https://sites.google.com/view/ppc-kadir-ider/home?authuser=1.

According to them, privacy control consists of the following elements (Joint Task Force Transformation Initiative, 2013, Appendix J p.2):

1. Authority and Purpose
2. Accountability, Audit and Risk Management
3. Data Quality and Integrity
4. Data Minimization and Retention
5. Individual Participation and Redress
6. Security
7. Transparency
8. Use Limitation

The following conclusions can be drawn from the requirements: Privacy control shall be designed to achieve compliant processing (systems) and user control.
Considering the GDPR requirements, the user-oriented privacy control must further comply with the principles of processing in accordance with Art. 5 GDPR. A mapping of the NIST requirements with the GDPR highlights the elements that are covered and where additional features are needed:

Table 6: Mapping of GDPR Principles and NIST Security Requirements

Art. 5 GDPR – Principles Relating to Processing of Personal Data	Mapping with NIST Security Guideline Principles
Lawfulness, Fairness and Transparency	covered by NIST guideline (7. Transparency)
Purpose Limitation	covered by NIST guideline (1. Authority and Purpose)
Data Minimization	covered by NIST guideline (4. Data Minimization and Retention)
Accuracy	no accurate matching; needs further specification
Storage Limitation	covered by NIST guideline (4. Data Minimization and Retention)
Integrity and Confidentiality	covered by NIST guideline (3. Data Quality and Integrity)
Accountability	covered by NIST guideline (2. Accountability, Audit, and Risk Management)

It is noticeable that the first NIST requirement, “Authority and Purpose”, lists the authority to collect as a sub-element (Joint Task Force Transformation Initiative, 2013, Appendix J p.2). Such a requirement is covered by Art. 6 GDPR, defined as the lawfulness of processing, which differentiates among six lawful bases:

1. Consent,
2. Performance of a Contract,
3. Legitimate interest,
4. Legal Requirement
5. Vital Interest,
6. and a Public Interest.

The only element that is not covered directly by the NIST security guideline is the accuracy element. According to Art. 5 (1) lit. d GDPR, personal data must be kept accurate throughout the entire processing lifecycle and rectified were inaccurate. Accuracy further requires the immediate deletion of personal information as soon as the purpose for the processing is fulfilled. Such requirements are covered indirectly by the NIST guideline (section 3), in particular the data integrity (section 4), especially the retention and disposal of data.

3.3.1.3. Technical Architecture

The preceding chapters identified minimum specifications for a compliant system. They include data subject rights, trustworthiness-building control features and technological security to meet the legal requirements arising from the GDPR. Based on the insights gained from the definitions, the subsequent analysis will translate such requirements into technical measures. This procedure may take place independent from the data analysis of surveys and studies, as this paragraph primarily lays down the technical infrastructure for the privacy control interface and discusses different options and their feasibility. Consequently, the UI/UX design as well as the interface content will be derived from the survey results.
The following technical architecture (Figure 7) shows a high-level summary of the to-be-workflow. It encompasses an end-to-end view of all interacting elements, thus, reducing the complexity of international data transfers. It includes (1) the data subject, which engages with the (2) user interface of the privacy control system, (3) the EU-based data centers that store the data in a GDPR compliant manner and (4) the organizations that process user information and are accountable for GDPR compliance as well as the (5) Application Programming Interface (API) service, which is a critical gateway to connect organizations with data subjects. Each of the elements (1 to 5) stated above will be decomposed and explained in detail with corresponding text and figures in the subsequent sections.

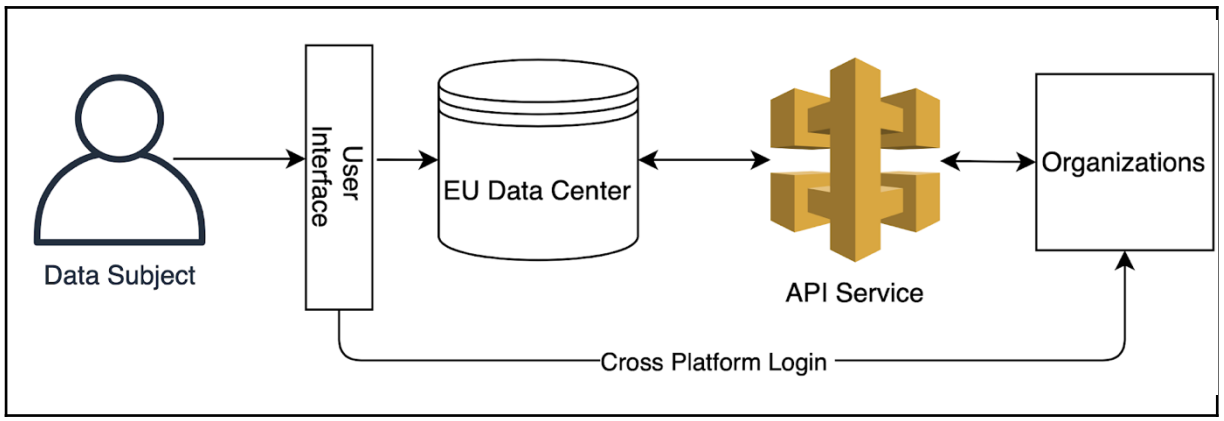

Figure 7: Conceptual Design of a PPC Workflow (Ider, 2020a)

An alternative option, provided in Figure 8, explores a design modification to decrease overhead data by a direct connection through API services. This allows the retrieval of data on demand. The concept shown below proves to be less invasive, due to the decentral mechanism. The upside of this privacy design feature is the decreased invasiveness and improved scalability, as the data processing organization is accountable for the storage and maintenance of personal information, leading to a more cost-effective solution. The downside is that once a user uses his/her right of data erasure ('right to be forgotten'), in accordance with Art. 17, the data will be permanently lost. Exceptions include data that must be retained for statutory purposes, which would need to be provided to the individual as well. Moreover, the technical and organizational security of the data may vary across the different data controllers. Consequently, data is secured, depending on the measures implemented by each organization. A design takeaway is that the privacy interface should provide a separate section, where all organizations are listed that hold data on deleted user profiles.

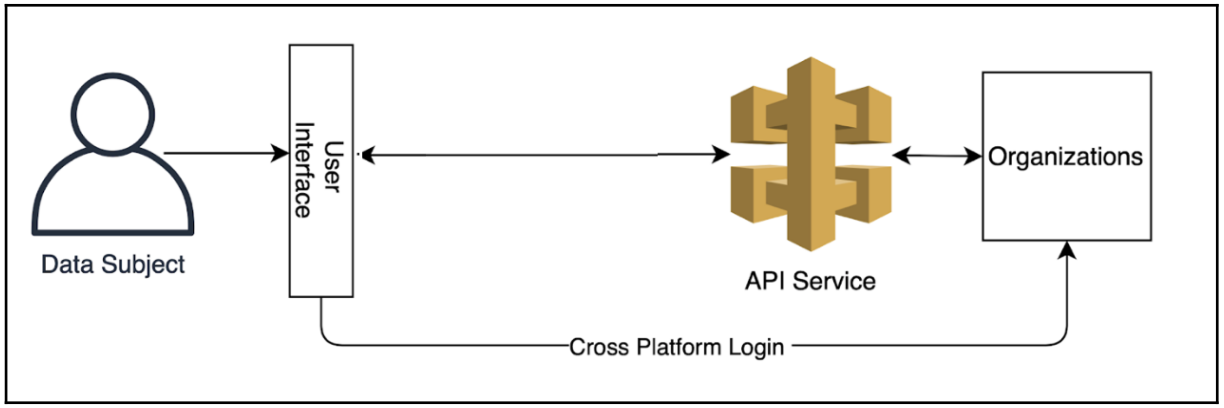

Figure 8: Conceptual Design Alternative of a PPC Workflow

Element 1. Data Subject

The data subject will be any natural person engaging with organizations and transmitting personal information in exchange for products and services. The GDPR based assessment of the term "user" highlights that each data subject has its user rights and therefore the designated interface should provide respective feature elements.

Element 2. User Interface

Individuals will see a single user interface for the management of their data. At the initial sign up, a unique personal identity (ID) number will be assigned to each user. The ID may further be used as an electronic personal identifier for authorization and various online transaction purposes. The main page structure consists of three segments, i.e., government and healthcare, social media, finance, and insurance. Each segment groups all organizations that process personal data and are connected to the privacy system.

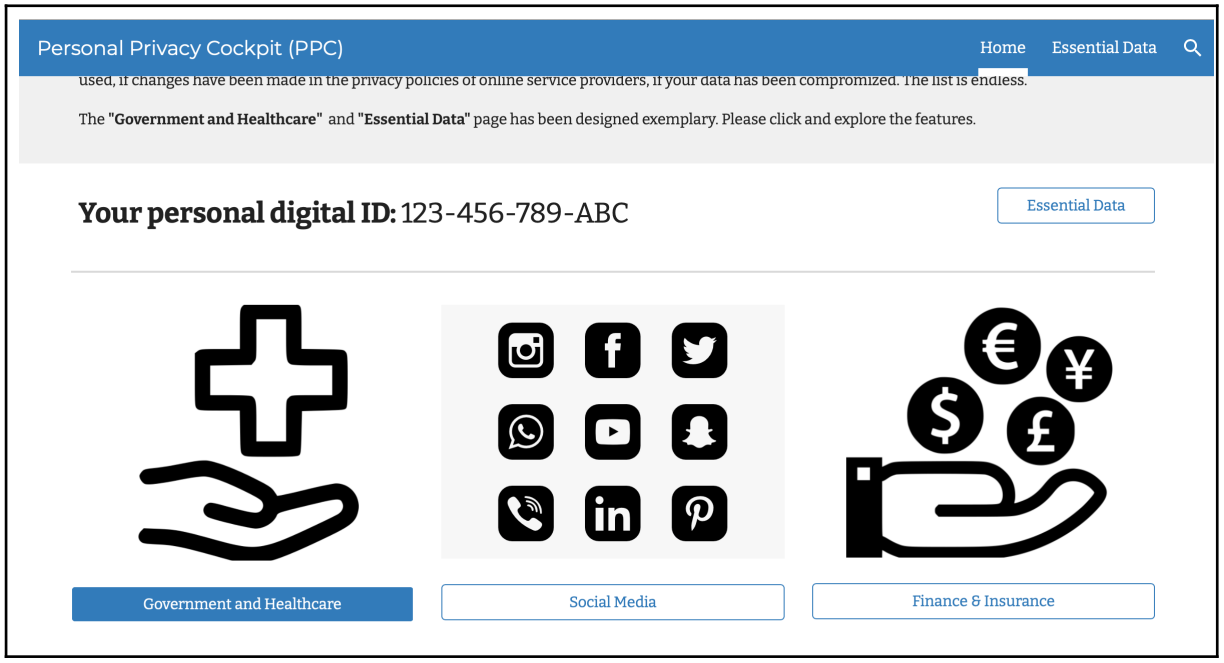

Figure 9: Mock-Up of PP User Interface, Homepage (Ider, 2020a)

A mock-up of the Government and Healthcare subpage is presented as exemplary in Figure 9 above. It details all organizations that hold personal information on the user. The interface is designed to minimize complexity for the user and concentrate on the relevant information features that allow effective communication of privacy modalities.

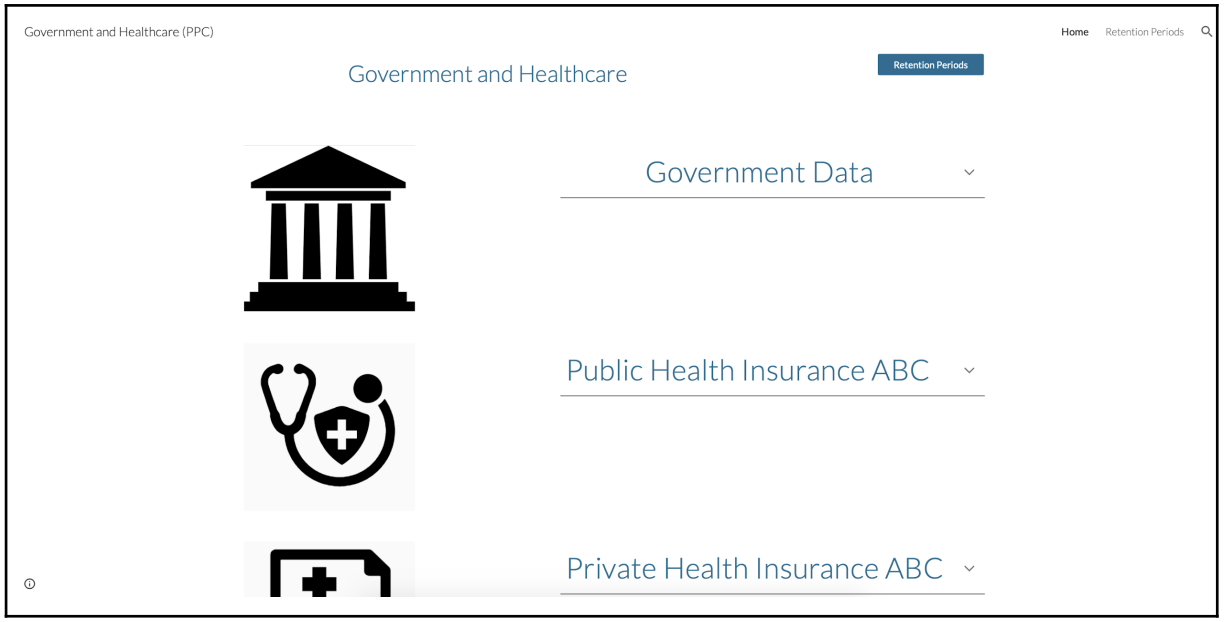

Figure 10: Mock-Up Government and Healthcare Landing Page (Ider, 2020a)

An expand and collapse function allows users to view the personal information, which organizations process, as displayed in Figure 10. This view satisfies the data access rights following Art. 12 - 15 GDPR. These articles require little to no interaction between individuals and organizations and are therefore static information. Consequently, Art. 17 - 23 GDPR requires active interaction between the two parties.
For example, data rectification or the request for data portability could be achieved through a service extension of the privacy system, allowing interactive communication. The preference will be further researched during the following chapters of this doctoral dissertation.

Figure 11: Mockup Government Data Categories Specifications (Ider, 2020a)

The Retention Periods subpage, presented in Figure 11, will provide specifications for the length of data storage, and meet the transparency obligations and fulfillment of user rights. The current setup foresees a separation of data categories and retention periods. An A/B testing procedure can verify if a consolidated view is more effective than the current setup.

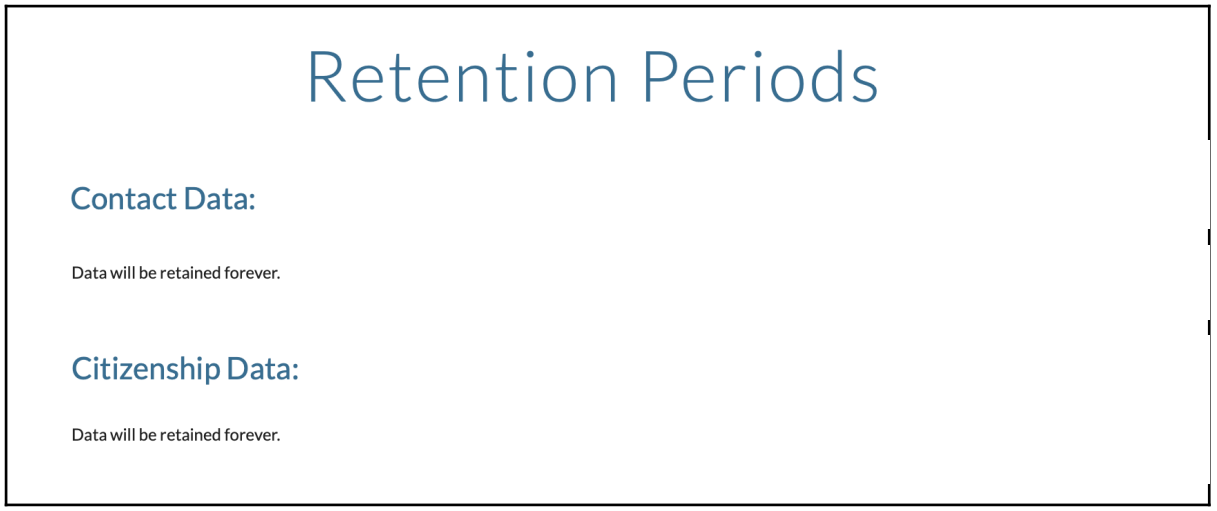

Figure 12: Mock-Up Government and Healthcare Retention Periods (Ider, 2020a)

Element 3. Organization

Organizations need to ensure the transmission of personal data on the internal system- and process-level in an industry-standard format. Common data formats are JSON (JavaScript Object Notation) and XML (Extensible Markup Language) (European Commission, n.d.).
As identified in the preceding chapters, Recital 68 of the GDPR "Right of Data Portability" already requires a machine-readable and interoperable format, which will not add additional implementation costs for GDPR compliance of organizations, as it is a prerequisite (Ider, 2020a).

Element 4. EU Data Center

EU based data centers ensure that any processed personal data of EU residents remains within the union. Consequently, such processing activities will be subject to the GDPR, and international data flows can be limited. This thesis proposes three alternatives, firstly, a government-led initiative to create a central data infrastructure and, secondly, an entirely separate data center for the management of personal information. The third option presents a solution that involves the hosting of an API service to a web interface.
Firstly, the Federal Ministry for Economic Affairs and Energy of Germany (BMWi) proposes a federated data infrastructure, which aims at decreasing the dependency on foreign critical digital technologies, safeguarding such strategic capabilities, and ultimately maintaining digital sovereignty of the data ecosystem (2019, p.6).
The proposal, framed as Gaia-X, foresees the establishment of connected data centers with centrally coordinated interfaces, data classification, interoperability and interconnectivity of data and processes between involved organizations (Federal Ministry for Economic Affairs

and Energy (BMWi), 2019, pp.14-15). This allows the integration of existing (cloud) infrastructures, thus, minimizing the disruption of such.
Data silos will be broken up, ensuring the integration of different cloud solutions into a single data hub architecture. Consequently, to centralize decentrally generated data, integrating with the user-centric data management system, decreases requirements and efforts for organizations to integrate with Gaia-X. A downside is that the project aims at big data integration, e.g., from manufacturing, sensors, a.o., thus, might require the labeling and separation of personal data in the databases.
Over the course of this research, however, the Gaia-X project remained in the idea phase and seemed not to move into the conceptualization (Vaske, 2022), which therefore limits its appeal to be considered as a viable choice for this research undertaking.
Nevertheless, in the scope of a conceptual appreciation, the user interface can accurately display the processed personal information, if connected to Gaia-X. However, a prerequisite is that the service goes live, and organizations integrate with Gaia-X.
xThe major risk arising from the integration is that the number of data categories is not limited to personal data but comprises IOT[13] device data linked or linkable to individuals. As the GDPR considers any data directly or indirectly linkable to an individual to be personal information, this imposes a more significant risk to individuals in the case of a data breach. Such a breach would allow attackers to jeopardize the privacy of individuals extensively.
The second alternative is to create a separate ecosystem for solely managing personal data, thus decreasing the amount of data stored in a single infrastructure. The primary purpose of the infrastructure is to create a central repository for organizations to share the collected personal data with the individuals via a central data hub. Such a data hub connects via APIs to existing databases of different organizations. This creates overhead data, as the existing information would be duplicated on separate instances, thus increasing risk exposure to individuals. Nevertheless, the risks are decreased compared to the Gaia-X proposal.
While both options require extensive hardware and software maintenance, the presented alternatives offer a viable and scalable platform to realize the online privacy control system. Figure 6 closely resembles this concept in a simplified flowchart, whereas “EU Data Center” may be replaced by Gaia-X or data hub respectively.

Element 5. API Service & Connectability to Various Systems

API services prove to be an excellent option for easy connectivity between systems, mainly due to its high usability for various purposes, such as deployment for the provisioning of data services or even to manage the authentication through a central directory (Osmanoglu, 2013, p. 470). Limits of its applicability and technology burden may occur at smaller organizations that do not have the capacities or resources to implement such an infrastructure. This could result in the incompleteness of the data presented in the privacy control center.

[13] IOT = Internet Of Things

3.4. Reliability models

3.4.1. Data Collection, Analysis & Evaluation Process

This chapter is dedicated to examining the data and its structure via a descriptive and analytical approach. Qualtrics Stats iQ will be mainly used, which features the visualization of numbers, ranks and categories.
The first section is dedicated to the methods of data collection. The second section contains a descriptive assessment of the data. 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.

3.4.1.1. 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 survey results are collected from the various platforms and merged in the Qualtrics system for detailed analysis. 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. Users are encouraged to share the link among their contacts. Two Amazon vouchers are raffled among the participants to incentivize further engagements and completions of the survey. The survey is shared on the respective platforms multiple times and cyclically to ensure consistent visibility on users' timelines. Both the Qualtrics and Google Forms survey links are kept active for 30 days. The target audience comprises individuals of all age groups from 18+, from different geographical, cultural, and professional backgrounds. Using various platforms for the distribution, the survey is set up to obtain more representative results. The actual audience is analyzed in the subsequent chapters to provide a transparent reflection.
Half of the questions, i.e., 13 out of the 25, are multidimensional, to capture multiple aspects of an individual. This design further facilitates data analysis on an aggregated and granular level. Subcategories of each survey question can be compared within and across other subcategories.

While the development of a privacy control system is suitable for global application and the data collection is carried out internationally, the examination of the collected data is not carried out separately for the EU respectively the European Economic Area (EEA) and the non-EEA countries. No significant response or preference deviations are observed in the examination of users from different regions.
Moreover, there is no differentiation made between the data collected via Qualtrics or Google Forms. The survey is designed to capture the user's perspective and consequently does not emphasize the preferences among an audience of a particular organization.
First, all data are analyzed together to ensure a holistic view. This is relevant to provide a global view of the privacy control system. In the second step, the data is segmented by pre-defined features, to allow a detailed drill-down and examination of any variances. The differences are then evaluated in the course of the analysis, to understand the impact on the privacy control system, which includes determining the trustworthiness of creating features and elements that enhance the users' control over their data. The preferences of the respondents are compared subsequently. Figure 13 depicts a sample evaluation for two subcategories of different questions. They relate to what extent users are comfortable sharing social information with how specific privacy features (here: detailed description of the privacy policy) would enhance the understanding of a privacy policy. In this case, the quantified answers are plotted in a crosstab and analyzed for statistical significance (1). The comparative subject matters are the willingness to share a specific data category and the extent to which the provided features enhance a privacy policy. The data is filtered and assessed by region: the European Economic Area (EEA) and its associated countries (2). The statistical test results are further depicted, as the evaluation shows a probabilistic significance (3). Lastly, the cross tab represents statistical significance, whereas the darker numbers reflect a higher proportion of users with the same answers (4). This methodological approach is used for data analysis. Thus, all statistical significance among the different answer options of subcategories will ensure full data validation.

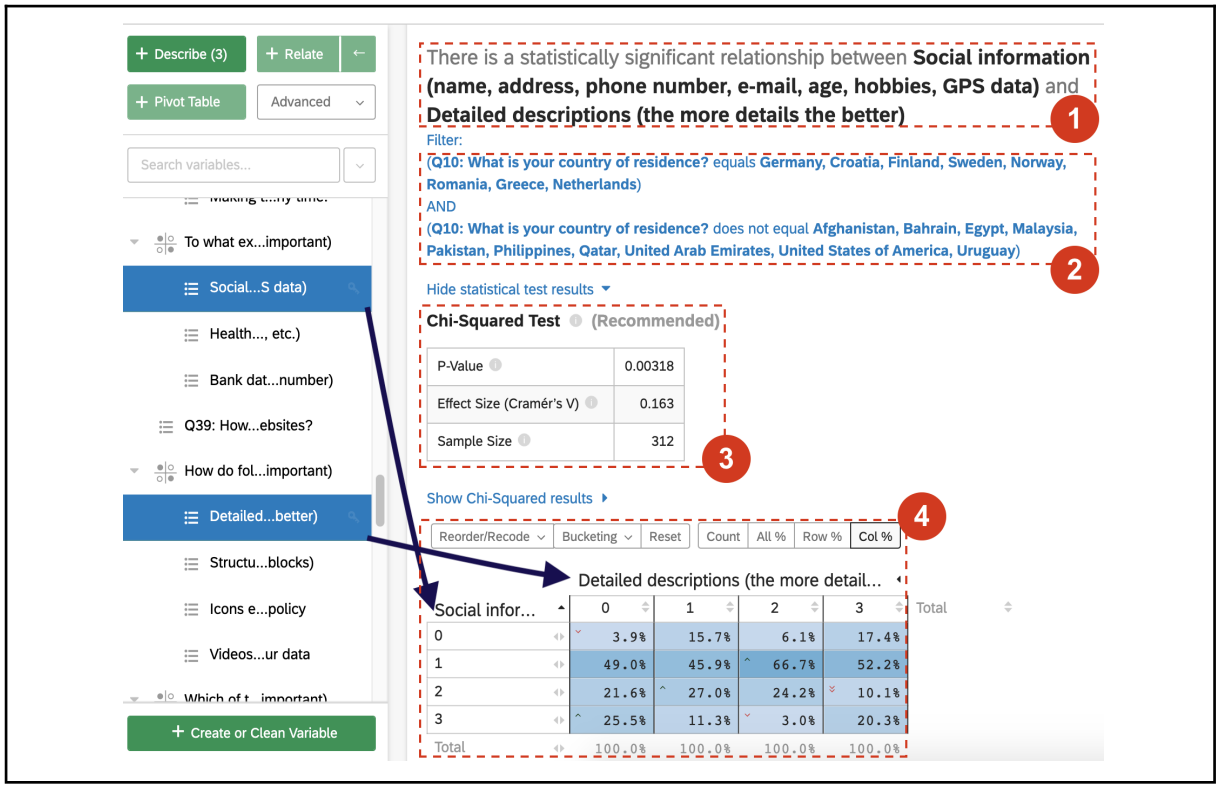

Figure 13: Extract from Qualtrics Data Analysis Tool

While the demographic questions on the first page are obligatory, users could skip subsequent questions or provide partial answers in the subcategories. The introduction section informs the participants on the subject matter, which includes:

- the understanding of the current level of confidence for sharing personal data with organizations,
- the determination of elements for reducing the complexity of privacy communication between organizations and users and
- the evaluation of trustworthiness building factors.

Furthermore, participants are informed that the results will be evaluated anonymously. The collected demographic data includes country of residence, age group, gender, occupation, the type and number of Internet-capable devices and an indication, if the device is personal or shared (device usership).

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[14] 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 trustworthiness-building matrix in chapter 2.3 Definition of Trust and Trustworthiness.
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 assessed through Text iQ, a built-in natural language processing service provided by Qualtrics.

3.4.1.2. 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.

[14] Questions will be asked in different sections.

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.
Other demographic questions, such as primary personal data, the exact date of birth, ethnicity, and accurate location, are not included in the survey, as they either directly or indirectly identify an individual. The individuals that provided their email addresses are not obliged, but free to do so, if they want to participate in the voucher raffle. By adding their email address and submitting the survey, users actively consent to the processing of their data for the indicated purpose, as shown below:

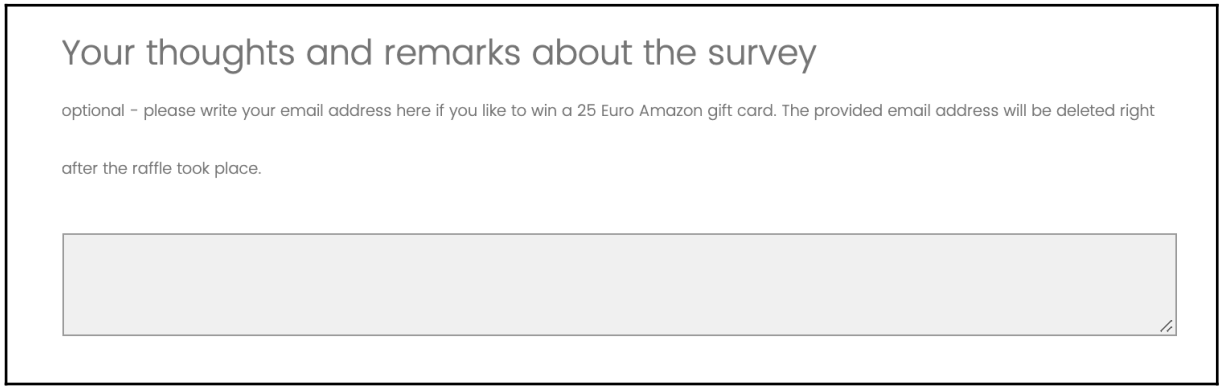

Figure 14: Optional Survey Question

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 and further conclude, whether the questions are comprehensible, relevant to the audience and indicate if the respondent is attempting to complete the survey as quickly as possible. This is a proposed survey method by Qualtrics (Qualtrics.com, n.d.). A visualization of the blank spots of the 431 survey responses is provided below for full transparency:

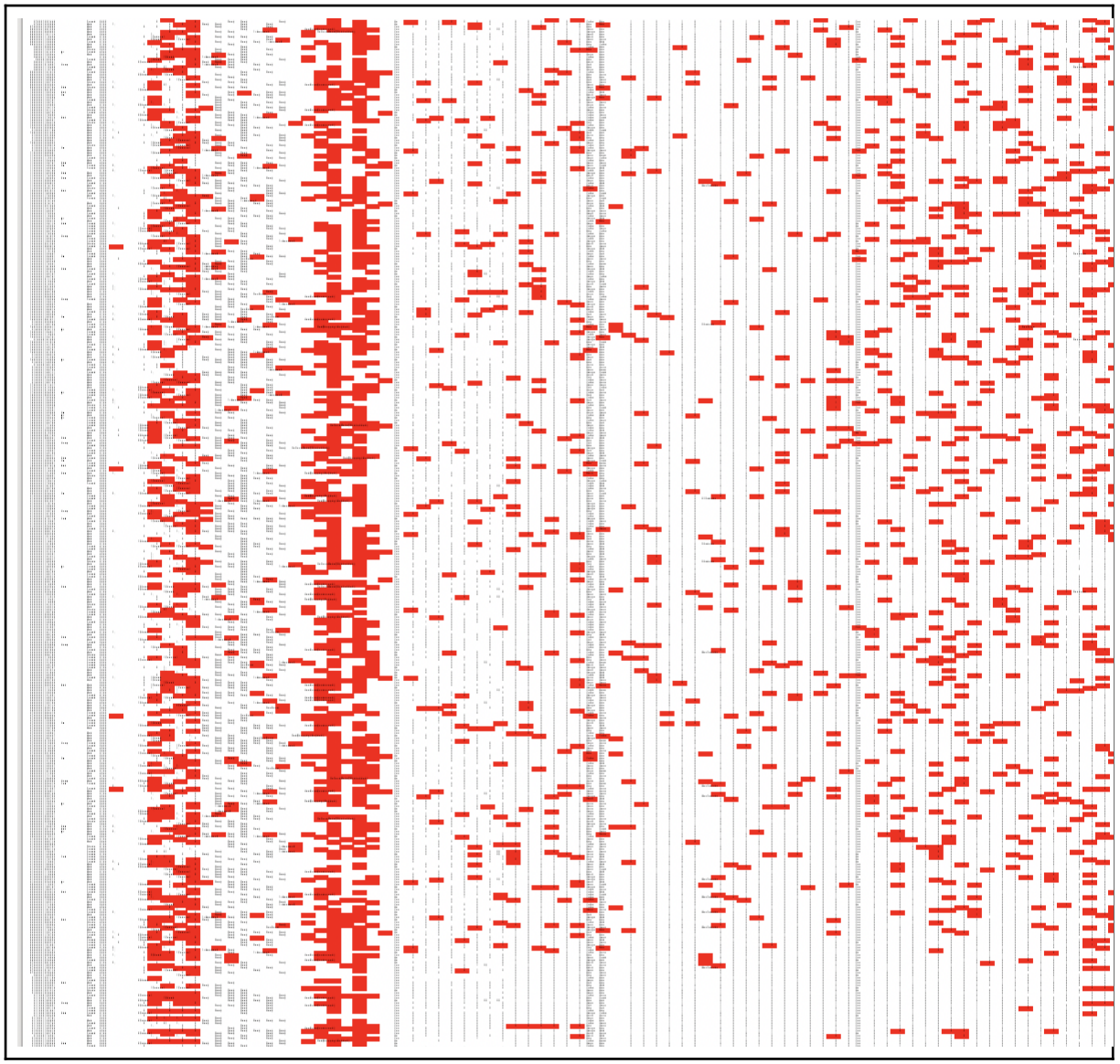

Figure 15: Visualization of Blank Survey Answers

Please note, blank spots (highlighted in red) do not decrease the quality and representativeness of the survey data. A blank cell may also indicate that respective respondents did not meet specific criteria, the answers were not applicable, or the respondent did not want to provide an answer. The type of questions, where this is possible is shown exemplary below:

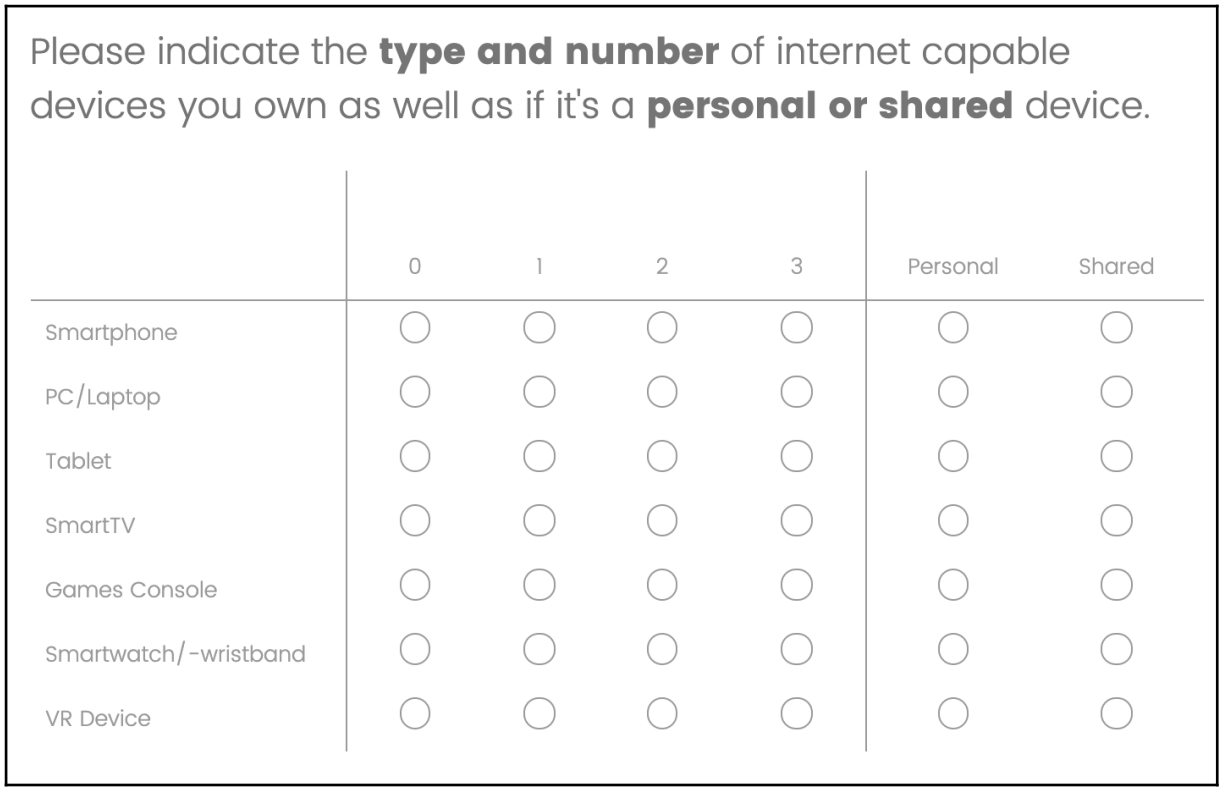

Figure 16: Sample Question of Survey

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. i.e., entire answers are removed from the dataset will not be considered, as it reduces the sample size substantially 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 7 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 7: 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[15]. 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.

3.4.1.3. Descriptive Data Analysis

The 431 survey participants reside in 18 different countries, where 57% live in Germany. EU respondents account for 76% of all answers. A benchmarking of responses of EU vs. non-EU individuals shows similar performance. Thus, during the analysis, no separate evaluation for both groups takes place. Agriculture and Natural Resources, Architecture and Construction and Government and Public Administration have not been selected out of the ten different occupation options. About 45% of all individuals across the different age groups have an occupation in Information Technology or Science, Technology, Engineering and Mathematics[16]. The second largest group accounting for 24% works in Marketing, Sales and Services and is therefore particularly interesting for the analysis as this occupation naturally requires more customer engagement where also large fractions of data subject requests are processed.
According to a Deloitte Digital report (Haas et al., 2019, p.16), roughly 50% of the most common customer-facing industries worldwide operate in either of the three top occupations. Therefore, it can be concluded that the collected data is valid and sufficiently represents the distribution of workforce across specified industries, as the following heat map depicts:

[15] Also, with the consideration that respondents seek to increase their chances of winning an amazon gift voucher.
[16] "Information Technology" and "Science, Technology, Engineering" are presented in a consolidated manner due to the proximity of the two professions. Differentiated view is provided in table 8.

Table 8: Heat Map Segmentation of Occupation by Age Groups [17]

	Age Group							
Occupation	20 - 25	26 - 30	31 - 35	36 - 40	40 - 45	46 - 50	51 - 55	Grand Total
Information Technology	35.29%	25.32%	19.42%	32.20%	23.53%		11.11%	24.59%
Marketing, Sales and Service	26.47%	25.97%	25.18%	16.95%	20.59%	50.00%		23.67%
Science, Technology, Engineering and Mathematics	11.76%	20.13%	23.74%	13.56%	26.47%	50.00%	44.44%	20.88%
Business Management and Administration	8.82%	14.29%	15.83%	11.86%	8.82%		33.33%	13.92%
Finance	14.71%	8.44%	9.35%	15.25%	8.82%			9.98%
Law, Data Protection	2.94%	5.19%	5.76%	6.78%	11.76%		11.11%	6.03%
Education and Training		0.65%	0.72%	3.39%				0.93%

The view shows the relative distribution of the data within each age group (i.e. column by column). This view allows the ranking of occupations per age group, while the total ranks the occupations across all age groups. Two of the three occupations with the highest row averages are strong quantitative academic disciplines. Thus, the survey responses are therefore analyzed separately for this group to identify whether their behavior in the context of exploring control perception and trustworthiness is different from the other occupational groups.

Potentially, personal data is diluted in shared devices, such as TV, tablets, or game consoles. Since multiple people share these devices, the risk for the collection of personal data is lower. The GDPR does not apply where there is no personal identifier, according to Art. 11. However, the same devices allow personalization through software or system configuration, i.e., the same interface may be customizable and thus personalizable through accounts and separate logins, where personal data can be obtained from. Despite the tendency to generate fewer personal information on shared devices than personal ones, it is essential to acknowledge that these mediums contribute to the increasing number of data collection endpoints. In total, 1612 devices are recorded, which corresponds to an average of 3.8 devices per capita. 85% of all respondents state that they share at least one device. Therefore, it can be concluded that most of the survey participants live in a shared household with at least one additional person.

This would mean, roughly 7 - 8 devices exist within a household of two people, validating the data published by the Federal Statistical Office of Germany (Statistisches Bundesamt (Destatis), 2020, p.44) and Audience Project's device usage report (Werliin & Kokholm,

[17] A table with absolute values is provided in appendix 1

2020, p.10). Smartphones (94%)[18] and computers/laptops (84%) are the most common devices owned by users. Tablets (67%) and game consoles (52%) are ranked on top of the shared for these particular device types and in comparison, exceed the number of personal devices. The percentages in all the cases represent the number of individuals owning a device in proportion to the number of responses (n = 431).

Table 9: Type of Devices Segmented by Usership

	VR Device	Tablet	Smartwatch/-wristband	Smartphone	SmartTV	PC/Laptop	Games Console	Total
Personal	8	64	162	405	161	362	86	1248
Shared	5	130	1	5	81	48	94	364

The insights generated in the preceding analysis conclude the following strategy: Due to many different answer settings, the data validation across and among various subsets of data (represented by the sub-questions) will exemplify devices that have the highest numbers in either segment. Smartphones and PC/laptops, tablets, and game consoles, respectively, will be validated in terms of sharing their personal data and the online interactions and behaviors.
The interim conclusion 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. 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 will therefore be 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.

[18] In the case of smartphones, the number is not at 100% as individuals may (1) not have answered this question or (2) still use a mobile phone, which is a different sub-segment among the mobile device types or (3) not own a mobile/smartphone altogether.

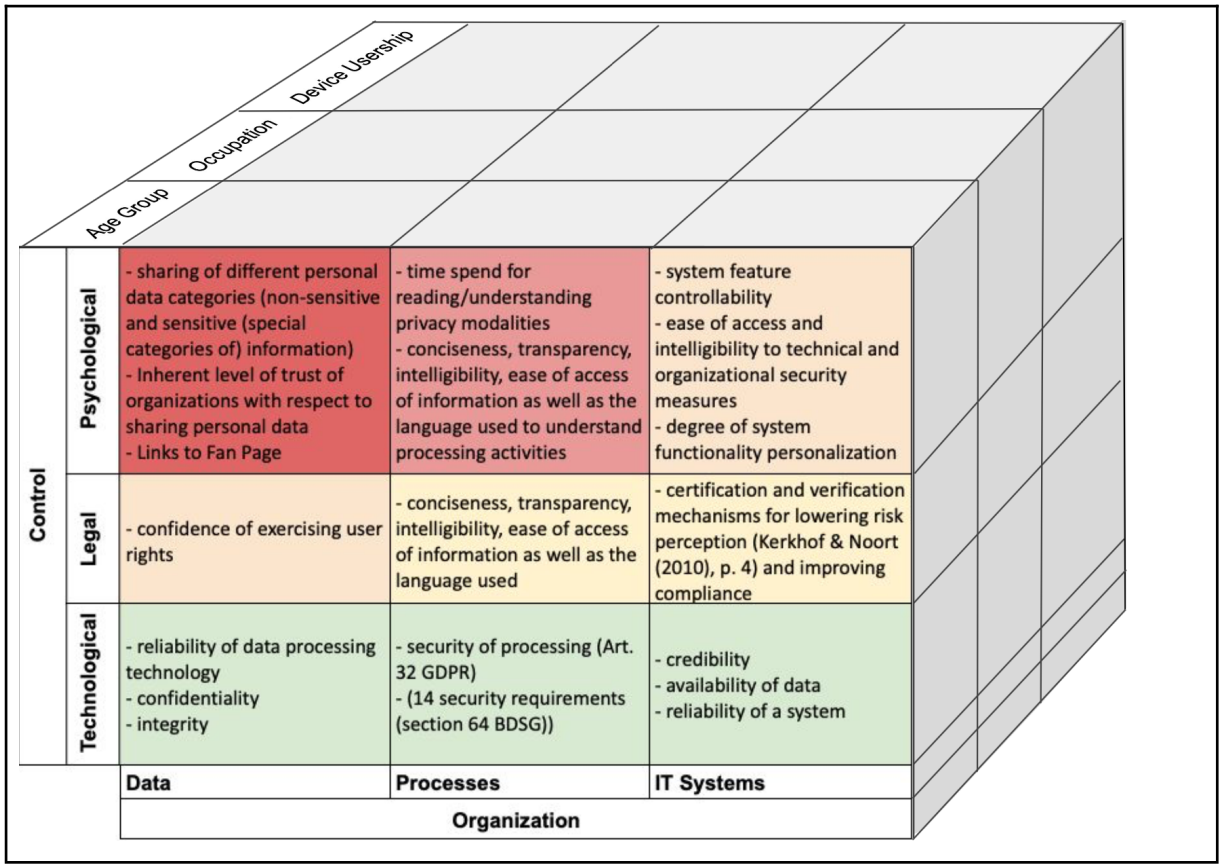

Figure 17: A 3D Concept of Trustworthiness Building Factors

3.5. Conclusion

In conclusion, this chapter presents a detailed description and analysis of the research methodology used to collect and analyze data related to users' privacy control system preferences. The survey was conducted through Qualtrics and Google Forms, and the data collected was analyzed using Qualtrics Stats iQ. The survey consisted of 25 questions with 84 subcategories, which were clustered into four sections. The first section explained the data collection methods, while the second section presented a descriptive assessment of the data. The third section explored the relationship between the responses, and the fourth section derived insights for the concretization of trustworthiness-building factors.

The analysis of the data was conducted holistically and then segmented by pre-defined features. The data was then filtered and assessed by region, and statistical significance was evaluated to ensure data validation. The survey targeted individuals of all age groups from different geographical, cultural, and professional backgrounds to provide a global and EU regional view of the privacy control system. The data analysis aimed at concretizing trustworthiness-building factors, which includes determining the trustworthiness of creating features and elements that enhance the users' control over their data.

4. Conditions and environment for implementing the solution

4.1. Creating a Successful Environment: Utilizing a Toolkit for Implementing Solutions

4.1.1. Data Evaluation Based on Age Group, Occupation, and device usership

Regarding psychological, legal, and technical control, the assessment of organizational aspects, including data, processes, and IT systems, are assessed by age groups, occupation and device usership in the following subsections. The outcome of this chapter provides insights on the level of control that exists and ways to improve control over the data from a psychological point of view. It will further provide information on the psychological impact of the trustworthiness of organizations and highlight if there are differences among respective segmentations.

4.1.2. Psychological Control Analysis

4.1.2.1. Psychological Control and Data, Processes, and IT systems

To assess the psychological control over data, the sharing behavior is analyzed in the first place. An analysis from the psychological perspective is conducted for age group, occupation, and device usership subsequently.

4.1.2.1.1. Age Group Segment Analysis

The bar chart below sums up all responses across the following data categories, clustered by age group and in absolute numbers. The bold

- Contact data (name, address, telephone number, e-mail, mailing lists)
- Non-health data (age, sex, weight, height, etc.)
- Lifestyle (interests, hobbies, taste, passions)
- Opinions and convictions (religious affiliation, political opinions, etc.)
- Web data (website visits, clicks, posts, likes, comments, cookies, etc.)
- Sensor data (smart gadgets, household devices, etc.)
- Location data (GPS data, etc.)

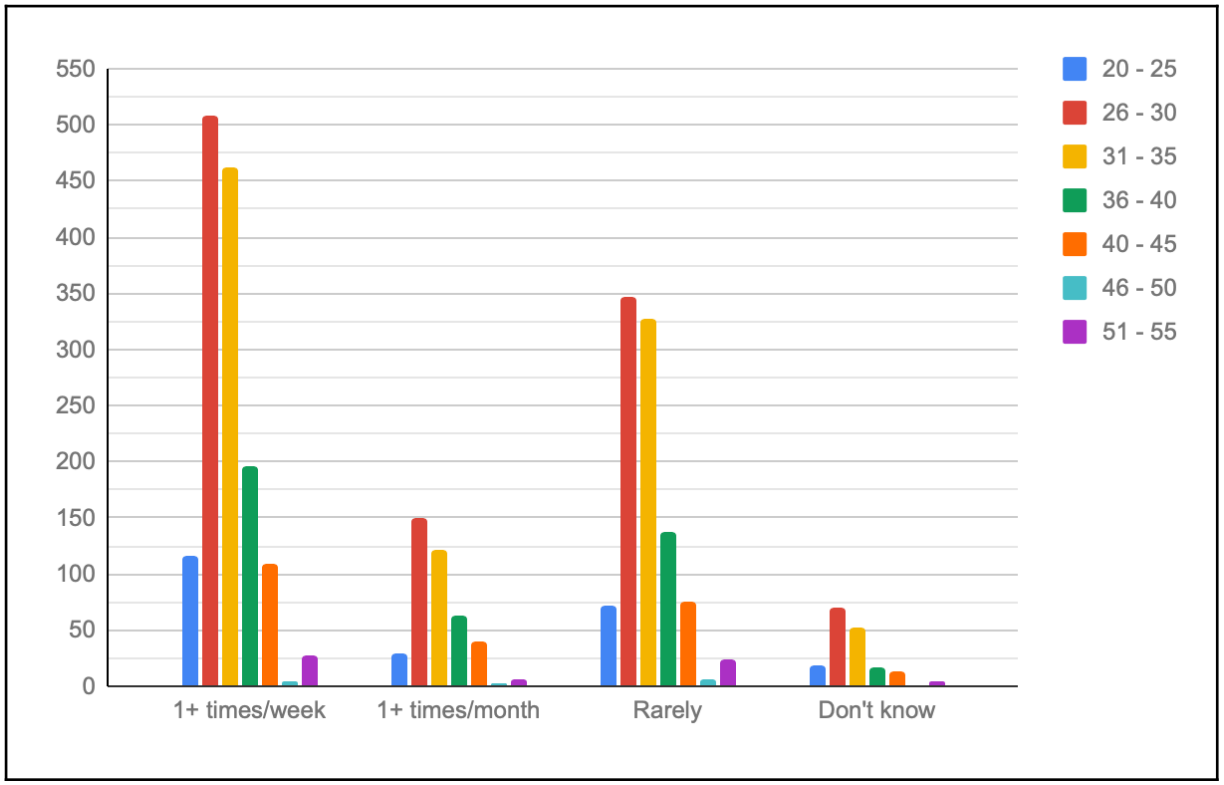

Figure 18: Data Categories and Sharing Behavior Clustered by Age Group

A granular heatmap is presented in appendix 2. The chart strongly suggests that most shared information comes from the age groups between 26 and 35, while most of the data is shared once a week or rarely. This distribution is in absolute but also proportional numbers. A validation question shows that users across all age groups tend to be more comfortable sharing non-sensitive data (highlighted in bold letters, see the list above Figure 18) while being more conservative in sharing sensitive information.

This observation is benchmarked and validated with a report that analyzes the most invasive apps and the personal data they collect from users (Dimitrov, 2021).

It is therefore appropriate to conclude that data types exert considerable influence on frequency and willingness to share such information with organizations. Thus, trustworthiness towards organizations is strongly influenced by the users' inherent perception of the sensitivity level of their personal data. Less sensitive perceived information tends to be more frequently shared, or there is a higher degree of openness to share such data and vice versa. This further validates the research results of Lewicki, McAllister, and Bies definition (1998, cited in Lyons et al., 2011, p.220). Trust represents a degree of certainty in a positive (i.e., trusting) context, which is the higher openness of users towards organizations for sharing certain data types, i.e., sensitive, and non-sensitive data. Although not directly defined in the survey, users naturally distinguished sensitive data from non-sensitive data according to the evaluated responses. While social information (name, address, phone number, [...], hobbies, GPS data) are not perceived as sensitive, other data, such as health information (medications,

sick notes) or bank data (bank account details, credit card number) are instead considered to be sensitive. This differentiation is entirely in line with the GDPR, which determines sensitive data in Art. 9 Processing of special categories of personal data.
The level of trust towards organizations is further analyzed by the features that would improve the trustworthiness of organizations, including:

- Conciseness of privacy information
- Transparency of data processing
- Intelligibility of privacy information
- Ease of information access (e.g., easy navigation and identification of specific privacy topics)
- Use of plain language.

The corresponding survey question is as follows:
Please indicate to what extent each statement would give you control over your data after sharing it with organizations (0 = not at all; 3 = very important).

The evaluation shows that these improve the trustworthiness of organizations, irrespective of age group, data type and sharing frequency. Considering the last two parameters, the breakdown of the data shows that for the non-sensitive data that are shared at least once a week, users perceive all trustworthiness building factors as equally important. The same observation is made for sensitive data, which is shared rarely. It shows equal importance for all trustworthiness building factors. Consequently, organizations need to put a special emphasis on the design of privacy communication features that meet such requirements. This must also be reflected in the privacy control system. While this assessment looks at the results across all age groups, a separate view on the age groups 26 - 30 and 31 - 35 that are part of the Millennials and Generation Z shows a more concrete result.
They rated the ease of information access, transparency of data processing and use of plain language particularly as essential features for achieving trustworthiness. Although the foregoing features are considered as crucial for the establishment of trustworthiness and psychological control over the data, the feature “Links (Icons) to Fan Page of organization (Facebook, Twitter, Instagram, etc.)” shows no significant effect as it's perceived less important across all age groups.
The psychological control over processes can be measured based on the time spent reading and understanding privacy modalities, the conciseness, transparency, intelligibility, ease of access of information, and the language used to understand processing activities. While they are partially congruent with the features defined above and clarify how important each of the features is, the focus in the subsequent assessment is to measure their actual effectiveness. The assessment of the processual understanding will take place across the different age

groups. Understanding the data processing from a processual perspective adds an even deeper layer of transparency and effective communication of privacy modalities.
This additional level of transparency may be necessary to improve user engagement with privacy modalities. According to the survey data, on average 60% of users tend to spend less than two minutes reading the privacy policy. Among the age group 40 - 45, the number is at 76%. The privacy policy is particularly important, as it represents the main source for individuals to comprehend organizational data processing activities. It answers fundamental questions on the Five W's:

1. Who is processing whom's data?
2. What (personal) data are processed, for what purpose, what means are used and what are the legal grounds?
3. When is it processed?
4. Where is the data processed, will the data be transferred across EU borders?
5. Why does the organization need to process this data?

A cumulative 92% of all respondents indicated that they spend between zero and a maximum of five minutes to read the policy. According to research study "The Cost of Reading Privacy Policies" (Mcdonald & Cranor, 2008, p.554), the average time to thoroughly read a policy is around 10 to 12 minutes for a medium or extended policy, respectively. This is only met by 8% of the respondents.
However, considering the trend that the policies have increased in length and word count since the GDPR took effect (Sobers, 2020), the average reading time shifts beyond the 10-minute mark. Under these circumstances, only 2.5% of respondents reported to effectively read the policy. On the other hand, users (n = 181) are asked in a separate study conducted in the scope of this research how much time they believe it takes to read an average privacy policy thoroughly. Around 68% believe that it takes 20 minutes to read the privacy policy, which is in complete contrast to the actual time spent reading, as displayed in the Figure below:

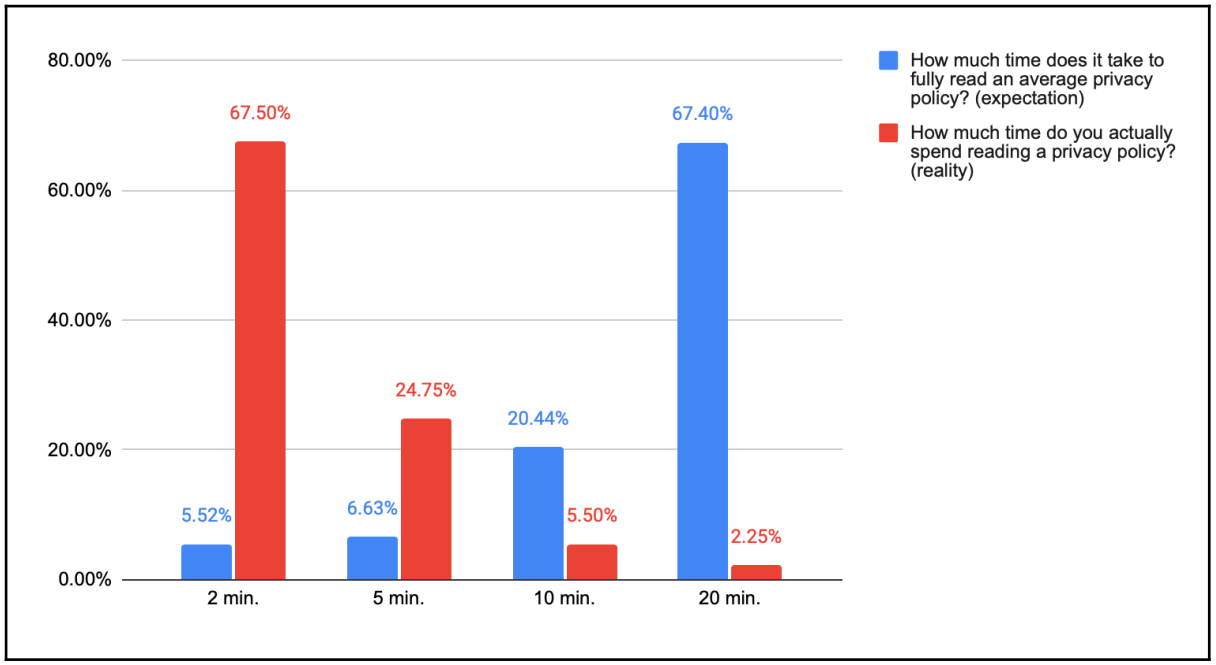

Figure 19: Time Spent Reading the Privacy Policy

This circumstance leads to low transparency and thus reduces the control perception of users over their data. The cycle completes with the decreased trustworthiness in organizations.
Reducing the time cost of reading policies could encourage users to read (Mcdonald & Cranor, 2008, pp.566-567). According to the data, online users are more likely to skim through policies than read them thoroughly. Therefore, privacy design features should be implemented to reduce the search for information, provide important privacy modalities in a nutshell that are easy to comprehend while allowing users to further drill down into the information. This meets user behavior and improves engagement with policies. After all, organizations are only as compliant as the users who can effectively understand the processing of their data.
The preceding findings are enforced by the assessment of the psychological control over data, processes and IT systems clustered by age groups, which reveals that the psychological control variables can be narrowed down to a few specific ones.
These are shown in the following table and are underpinned by color. On the spectrum, green areas represent the lower end while red represents the upper end.

Table 10: Most Impactful Control Features are Segmented by Highest Rated User Statements

	Transparency of data processing	Ease of information access	Use of plain language
It is important that organizations always ensure that my data is accessible for me (e.g., via a user account).	52.00%	53.80%	49.70%
It makes me more confident to have control over my data, If organizations (internally) have strict data access policies	48.90%	60.30%	56.50%
Control over my data is strongly connected to concise, transparent, intelligible, and easily accessible privacy information	50.30%	57.10%	57.80%

The view considers the information provided by the two age groups Millennials and Generation Z in total, as these make up most of the respondents (70%) and therefore have a particular influence on the overall analysis and results. Consequently, the highest ratings for each respective feature, i.e., transparency of data processing, ease of information access and use of plain language are cross-checked with the highest values of the statements that would give users most control over their data after sharing it with organizations. The concrete question is as follows: Please indicate to what extent each statement would give you control over your data after sharing it with organizations (0 = not at all; 3 = very important).

Based on a column-wise assessment (n = 431), the table shows that there is an association between the transparency of data processing with the statement “It is important that organizations always ensure that my data is accessible for me (e.g., via a user account)”. It is therefore confidently asserted that control and trustworthiness can be mutually achieved through transparent data processing and data accessibility. While the crosstab relationship of these particular parameters reflects the highest value based on the column view, the strongest relationships are found among ease of information access and use of plain language.

A crosstab of “Ease of information access” and the statement “It makes me more confident to have control over my data, if organizations (internally) have strict data access policies” show the strongest relationship, with 60% of respondents answering this as very important.

Information on access policies should therefore be implemented in privacy communication and easily accessible, e.g., through highlighting this as a separate subsection.

Particularly the improvement of easier information access may also have a direct impact on the transparency of processing, as data accessibility may further increase the transparency and thus improves the confidence over the control of personal data.

Ease of information access must be understood as (1) easy navigation through the web page for the purpose of accessing privacy modalities and (2) reduction of the complexity of the presented privacy modalities (e.g., policy).

Best practices according to the Guidelines on transparency, published by the Article 29 Working Party include just-in-time notices (Working Party, 2017, pp.19-21), incorporating layered methods but not merely nesting subpages.
Furthermore, considering the collection of data from devices without a screen, e.g., IOT products, ease of information access may be provided through a hard-copy, URL link or QR code (Working Party, 2017, p.12). A combination of such methods would further ensure ease of information access through the facilitation of different channels and ultimately, leading to adherence with the GDPR. Thus, designing the interface in a manner that minimizes the complexity of adequate information access, i.e., communicating the relevant privacy modalities just before the data collection, provides an effective feature for improving control and trustworthiness.
The privacy control system could either mirror organizations' privacy policy or facilitate such a drill down and roll up functionality for improved control over the data. Nevertheless, it is ultimately the legal obligation of data processing organizations to ensure the effectiveness of their privacy communication.
The third pillar for control and trustworthiness over the data is represented by the usage of plain language and “Control over my data is strongly connected to concise, transparent, intelligible and easily accessible privacy information”. This crosstab relationship can be understood as a validation of the foregoing control features as it reinforces the requirements and preferences of respondents. It is further noticeable that there is an almost equivalent number of users that associate the usage of plain language with strict data access policies.
Although the foregoing definition focuses on the legal aspects, it cannot be ruled out that the respondents may construe the statement ambiguously. Strict data access policy can therefore be further understood as data access control that is in the power of the individual user, rather than organizational access control. Looking at this circumstance from the user's view, it can be drawn with certainty that the provisioning of data access services or features and maintaining a simple language, would increase the control and trustworthiness of the most impactful features to the same degree.
It can be concluded that the ease of information access possesses the highest leverage effect on the control and trustworthiness, with respect to the assessment of the age groups.
Particularly the psychological control over processes and IT systems are the least tangible and thus most challenging elements to control and consequently, to build trust for.
Chapters 5.4.2. Legal Control and Data, Processes, and IT systems and 5.4.3. Technological Control and Data, Processes and IT systems are dedicated to further examine the features from a legal and technical perspective.

4.1.2.1.2. Occupation Segment Analysis

The subsequent analysis will further identify psychological control preferences and behavioral patterns over the data, processes, and IT systems, segmented by the occupation of

respondents. Figure 20 shows the frequency of sharing behavior of data based on the occupations, irrespective of the data types. For details on the data categories, please see section 5.4.1.1 Psychological Control and Data, Processes, and IT systems.
All occupational groups have one common feature, they most frequently share their personal data with organizations at least once a week, compared to all given options. At first sight, three occupational groups in particular, i.e., (1) Information Technology, (2) Marketing, Sales and Service and (3) Science, Technology, Engineering and Mathematics (see Table 8 for details) seem to stand out in all segments. However, it should be noted that precisely these three occupational groups are among the most selected ones overall and therefore show proportionally the highest values in all segments.

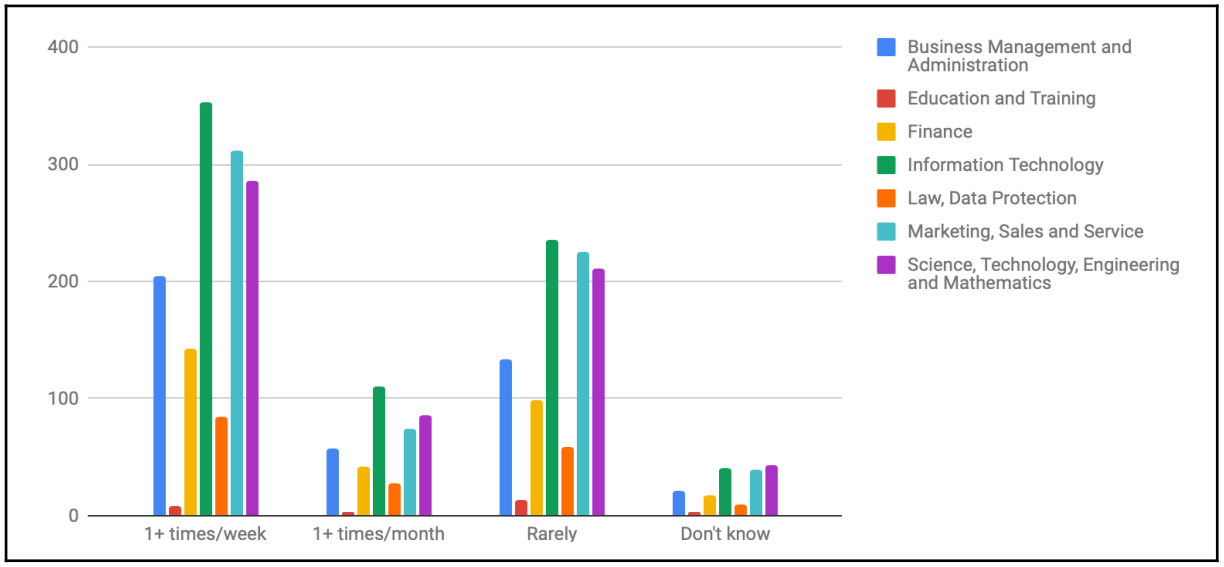

Figure 20: Data Categories and Sharing Behavior Clustered by Occupation

A drill down into the dataset reveals that individuals across all occupations have similar data sharing behavior. Location and web data are in both groups the most frequently shared data in this rank order (see table 11). Affected occupations below are grouped by two tiers, group A consisting of the three largest occupations and group B reflecting remaining ones:

- Tier A
  - Science, Technology, Engineering and Mathematics
  - Marketing, Sales and Service
  - Information Technology

- Tier B
  - Business Management and Administration
  - Education and Training
  - Finance

- Government and Public Administration
- Law, Data Protection.

Table 11: Tier A and B Proportional Data Distribution

Data Type	Tier A	Tier B
Location data (GPS data, etc.)	51%	34%
Web data (website visits, clicks, posts, likes, comments, cookies, etc.)	42%	28%

Excluded from the statistics are the following occupations due to insufficient and unrepresentative data[19]:

- Agriculture & Natural Resources
- Architecture and Construction
- Education and Training
- Government and Public Administration

The findings on the occupations reinforce the insights generated in the heatmap (table 8). Additionally, there is a homogeneous distribution of data sharing behaviors across all occupations. Particularly, location and web data are most frequently shared. Since the preceding chapter has highlighted the largest age group, i.e., 26 - 35 (consolidated view, consisting of two groups) and in consideration of the Tier A group it can be expected that a substantial amount of data collected and processed by any given organization will include web and location data.
A crosstab analysis with nine statements further reveals that individuals across all occupations ranked following viewpoints as most critical with in association with the sharing of the respective data categories:

Table 12: Average Consensus Rates of Top-Rated Statements

Statement	Rating
It is important that organizations always ensure that my data is accessible for me (e.g., via a user account)	71%
Control over my data is strongly connected to concise, transparent, intelligible, and easily accessible privacy information	69%
I prefer detailed (extensive) information on the technology used in an organization	68%

[19] It cannot be ruled out that survey participants may have selected an occupation, other than their actual one.

A similar behavior has been identified in table 10. It can therefore be deduced that the clustering of data by occupations shows a strong correlation in terms of the assessment of psychological control preferences. The importance of data access, thorough explanation of processing activities (use cases for the data usage) as well as the underlying technologies, while providing the information in an easily consumable mode.
The importance for organizations to provide information on data categories in the respective manner becomes even more evident through the analysis of the trending imposed GDPR fines. A filtering of all 477 imposed fines shows that roughly 10% of all fines are associated with keywords, incl. location, GPS, website, and cookie[20] .
A web scraping analysis of fines in 2021 shows an increase of almost 8 percentage points, amounting to 18% of all imposed fines. The criteria used for the analysis are equivalent to those stated in the paragraph above.
In both instances, i.e., in the data until December 2020 and from January 2021 shows that 70% of the underlying violations are attributable to insufficiency of legal basis for data processing and lack of fulfillment of information obligations, whereas the remaining 30% are due to insufficient technical and organizational measures. Particularly the lack of legal basis and inadequate information provisioning, which both have a strong causal relationship, are of importance as they are customer facing. Therefore, the privacy policy of organizations and the privacy control system should have an easy access and dedicated section to information on the usage of web and location data.

4.1.2.1.3. Device Usership Segment Analysis

The third dimension of analysis is the assessment of device usership to identify further psychological control preferences and behavioral patterns over the data, processes, and IT systems. Device usership refers to the possession of different internet capable devices.
The data does not differentiate between personal or shared devices as the primary interest is the general understanding of sharing behavior, irrespective of the circumstances of the device usership.

[20] Data last recorded on: Dec. 31st, 2020

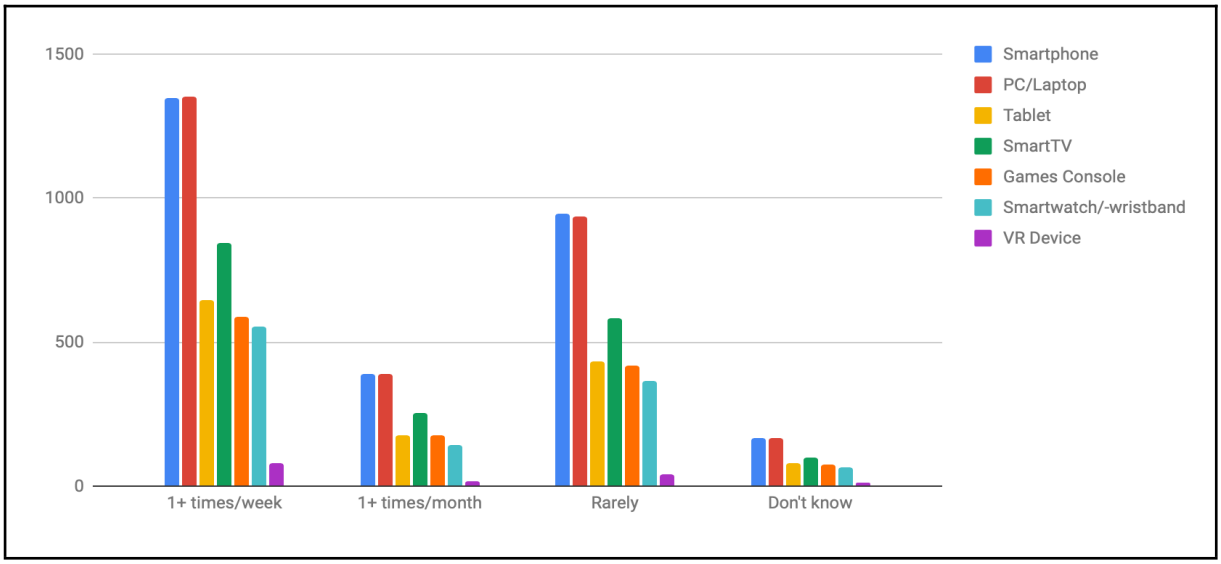

Figure 21: Data Categories and Sharing Behavior Clustered by Devices

A similar pattern of the plotted data in Figure 21 is observable in Figure 20. Most frequently used devices, i.e., Smartphones and PC/Laptops show the most frequent sharing patterns. Over 94% of individuals share their data via the devices stated in Figure 21 at least once a week, a month or rarely, while 6% did not or were unable to provide any information.
Of all respondents (excl. "Don't know"), approximately half share their data at least once a week. Personal information disclosed via the top two devices, Smartphones and PC/Laptops, account for 45% of data within the sharing frequency once a week (i.e., 1+ times/week in Figure 21) across all device types, while these two devices and frequency account for roughly 25% in proportion to the sharing frequencies 1+ times/week and month, rarely but excluding "Don't know". A summary of the Figures is presented below:

Table 13: Data Sharing Frequencies, Segmented by Devices

Sharing Frequency	All Devices	Smartphone and PC/Laptop Combined
1+ times/week	50%	45%
1+ times/month	15%	40%
Rarely	36%	40%

This ascertains the need to develop a UI friendly privacy control interface for such devices but for Smartphone and PC/Laptops. The data analysis confirms the major findings in the preceding chapters with regards to features that enhance psychological control over data and establish trust towards organizations, as summarized in table 10. It can further be concluded that many control elements and trustworthiness building factors will primarily enhance interfaces for the two prime devices Smartphone and PC/Laptop.

4.1.2.2. Psychological Effects of Colors

Colors matter in the development of a user engaging system (such as the privacy control system) as it is one of the first characteristics users recognize and engage with when visiting an organization's web page (Desnoyers, 2011, p. 150). Moreover, colors further represent an important design strategy as contrasting foreground elements with backgrounds enhance the accessibility to information (Mackiewicz, 2009, p. 8). Research proves that color has an impact on the trust users place in a website (Desnoyers, 2011, p. 156) and that the website and the underlying brand or organization are mutually dependent (Desnoyers, 2011, p. 150).
The reference study, "Toward a Taxonomy of Visuals in Science Communication" by Desnoyers (2011) (hereafter: study_1) refers to the measurement of the initial trust a user has when visiting a website. In study_1 an identical website has been presented in different colors to an audience, with various occupations.
The results indicate that depending on the occupation, users have different perceptions on the association between color and trustworthiness. Although the overall effect on trustworthiness is small, it still has a statistically significant impact, thus, to be considered as a valid input parameter for the psychological assessment of trustworthiness.
The comparability of study_1 and the survey conducted in the scope of this research (hereafter: study_2) is well comparable, as both studies match most colors and analyze the results by various segmentations, i.e., occupation. Colors in both studies are almost identical, main differences are that study_1 excluded pink but in addition offered turquoise and gray. However, both colors do not exhibit statistical significance in the outcome of the study. The option "no idea" is available in the reference study_1, while labeled as "none" in study_2. Study_2 will further investigate the effects based on age groups and device usership. The sole drawback of study_2 is that it did not present the websites in various colors but only the color set, shown in Figure 22.
Survey participants have been asked the following questions in this order and presented with the color table below:

- Which color improves your emotion/makes you feel positive?
- Which color do you associate with trustworthiness?

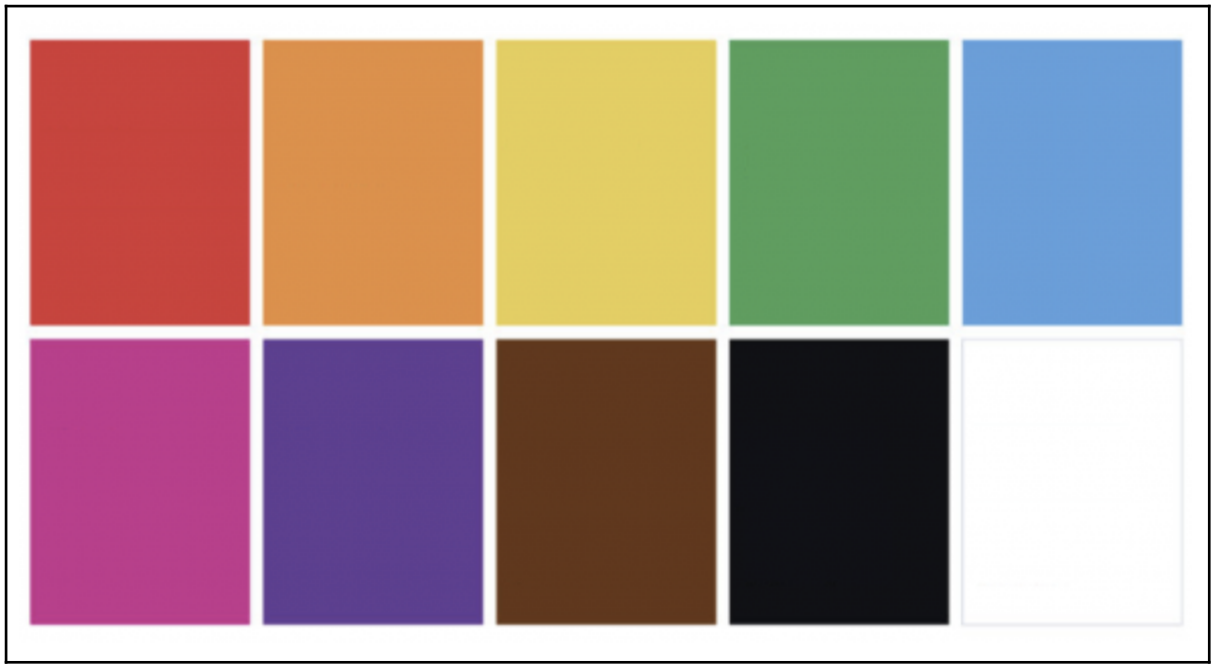

Figure 22: Color Table for Measuring Effects on Trustworthiness

Both questions have been asked to eliminate ambiguity among respondents. The survey answers identify a difference in the color perception, depending on the question asked.
The most frequently selected color in the scope of the question, which colors improves emotions, is yellow and is closely followed by green, both are equally represented.
At some distance from the top two but clearly above all other possible alternatives is blue. This observation is present in all segments in study_2, i.e., age groups, occupation, and device usership.
Contrary, the results of the question, which color is associated with trustworthiness shows a different order of color preferences as depicted in Figure 23. Blue is the most trustworthy color with an average score of 43.20%, followed by green with 24.46% respectively. The average scores refer to the responses clustered by age groups. Across all respondents in study_1 blue was selected as the most trustworthy color as well (Desnoyers, 2011, p. 157).

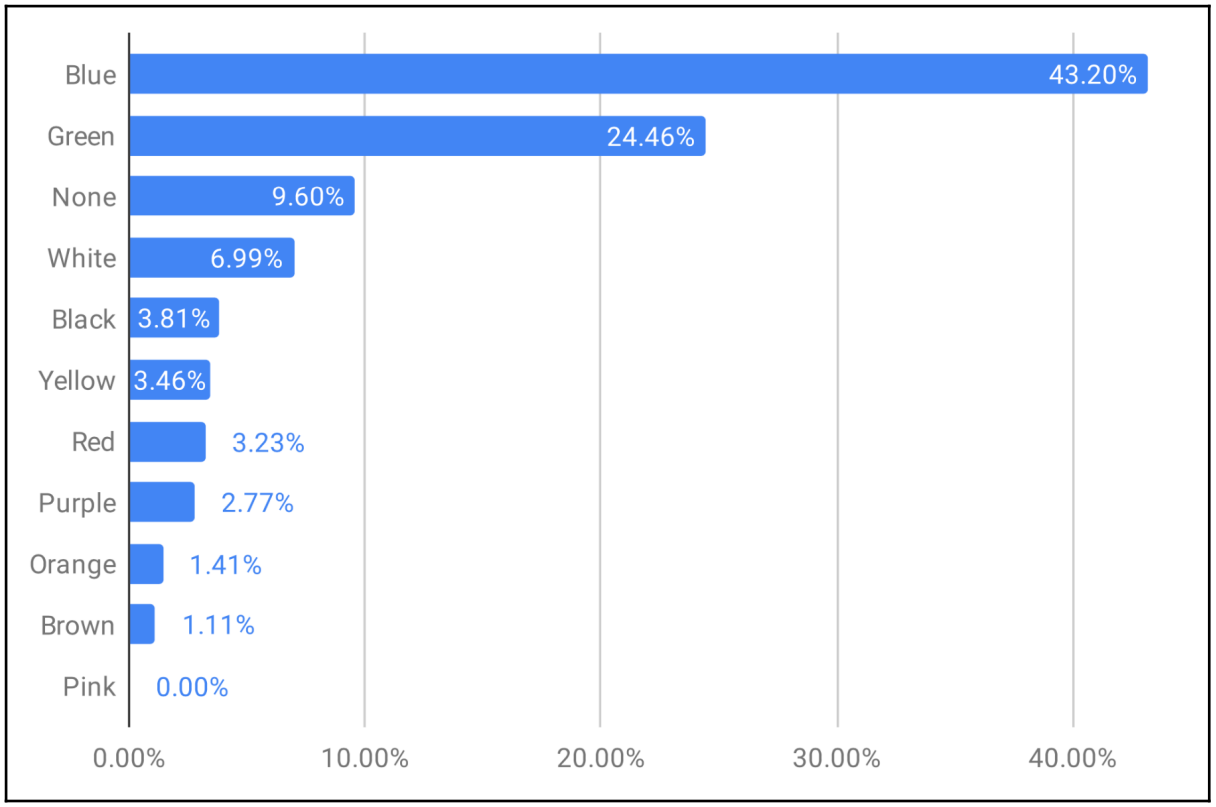

Figure 23: Trustworthiness-Building Colors Clustered by Age Group

As a reference, Figures 9, 10, 11 and 12 depict sequences from a mockup version of the privacy control system, designed solely in blue. Empirical evidence shows that blue promotes relaxation, reduce distress, which in turn lowers the risk aversion (Su et al., 2019, p. 271). Based on the associative learning theory, individuals link blue to peaceful and tranquil objects (Su et al., 2019, p. 271). Similarly applicable to the color green, but not to the same extent as blue.

A study shows that the introduction of green increases the confidence in the likelihood (Wasaya et al., 2021, p.13420) of a transaction. This encourages customers to get more involved with organizations e.g., reflected in the purchase of products or services. Applied to the control system, this feature provides the user with an environment that is even more trustworthy. Therefore, a key insight from the color analysis is to redesign features and add green elements into it.

While this survey analyzes the sole effects of colors on individuals' perception of trustworthiness, it is important to highlight that organizational attitude is positively affected by the introduction of new green products (Olsen et al., 2014, p.134) as well. Brand attitude is reflected in the improvement of product-related attributes, product category associations, symbols, advertising, and other marketing efforts. This effect is observed for younger organizations, as they are not yet established with their brand and colors.

While the introduction of green may improve association with more environmentally friendly and sustainable organizations (Pacer et al., 2017, p.162) it parallelly has a beneficial effect on the elevation of the trustworthiness-baseline of users, which is discussed in the section user suspicion towards IT systems and effect on trustworthiness in chapter 5.2.2.1. Technological Control and Data, Processes, and IT systems. The introduction of the color green into the privacy control interface may therefore decrease the suspicion towards IT systems and in turn the initial level of trustworthiness through the improved its appearance.
Nonetheless, a limitation of the applicability of specific colors to a centralized privacy control system may arise due to a conflict of interests. If organizations connect to a central privacy interface, it will not reflect their corporate colors (and other features like fonts) but merely maintain the color mostly associated with the centralized privacy control system, i.e., blue, and green as these are mostly associated with trustworthiness. This could be a roadblock for organizations to integrate into a centralized privacy control system as their brands may have a strong association with specific colors. A possible solution is to maintain colors and other features (e.g., fonts) of an organization. Both Figures below represent a mock-up version of such a solution. Figure 23 lists six exemplary organizations that are subject to the GDPR and process personal data of individuals and therefore integrate with the privacy control system. Thus, their logos appear in the control center. Figure 24 maintains the corporate colors and other features of "Organization A" when opening a deep link.

Figure 24: Control Center Listing All Organizations [21]

[21] Logos are self-designed

Figure 25: Details of Processed Personal Information

4.2. Conclusion

The various crosstab assessments in this chapter revealed that across all three segments, i.e., age groups, occupations, and device usership the psychological perception of control has almost an identical behavior.

In all segments, users show equivalent preferences when it comes to the sharing of data, ensuring control over data as well as the conditions that create trustworthy circumstances. This insight strengthens the data quality and the findings, showing a consistency across the different segments.

To ensure a 360-degree view, the perception of control and trustworthiness over processes and technologies were analyzed besides the data. The assessment shows that a substantial number of individuals spend insufficient time to understand underlying processes, processing activities and technologies, which limits the transparency for users to adequately achieve a confident level of control. Respondents show exactly these concerns, reflected in the answers provided based on attributes that could help them better understand the technologies that companies use to process their personal data.

The insights of all crosstab assessments are manifested in the engagement preferences with technologies. It seems that the decrease of technology suspicion and thus increase of trustworthiness of organizations and control over data can be improved through features, i.e.,

- Use of plain language (of all information provided to you)
- Ease of information access (e.g., easy navigation and identification of specific privacy topics)
- Transparency of data processing (What does the technology do with my data?).

Ultimately, psychological control over data, processes, and IT systems over data across age groups, occupations, and device usership strongly correlate with the provisioning of simple UI/UX and easy intelligible information. Moreover, access to information on frequent data categories, here represented by web and location data, must be designed to be particularly user-friendly and accessible.

The privacy control interface may integrate basic text mining features to identify, cluster and offer end users an easy method to centrally identify data categories and their usage frequency. Based on the frequency of word occurrences within a policy, the dashboard could display such categories and highlight their appearance within the policy. Existing services, such as Google Cloud Natural Language API come with a variety of services and provide integratable features. Such can be used to provide a summary engine for creating a short abstract of the whole policy, automated highlighting, and key feature extraction of legal grounds and/or data categories.

Using this method could solve an integral problem of many policies, i.e., the length and incomprehensibility of policy text, which prevents users from reading the information adequately, thereby reducing the effectiveness of data protection.

5. Experimental verification

5.1. Selection of an object for conducting the experiment

5.1.1. Legal Control and Data, Processes, and IT systems

The legal control evaluates the survey responses with regards to the effects of laws (here: the GDPR) and legal frameworks on the control capabilities of individuals on the three main subjects, i.e., data, processes, and IT systems. Due to the homogeneity of data for the age group, occupation, and device usership segment, the subsequent analysis will be based on the age group segment as this segmentation is also used by reference studies to measure trustworthiness (Gul, 1983, Ashraf et al., 2006). Existing deviations will be highlighted in each section respectively. The age group-based assessment of the legal control features will identify to what degree control and trustworthiness is affected by such statutory specifications. This will be achieved through an individual analysis of data, processes, and IT systems respectively. It further discusses the constraints, i.e., limitations, the legal requirements placed on control and trustworthiness. The analysis and evaluation of this subsection will ultimately provide insights (1) if or (2) if not and (3) to what degree age groups control over their data is or can be achieved through compliance with legal control mechanisms.
First, the confidence to exercise user rights across various age groups will be evaluated. The user responses undergo a holistic evaluation, i.e., (1) across all age groups and (2) across all user rights. The responses of each user right will further be discussed separately per age group.
This allows the identification of behavioral or preferential differences as well as understanding the effect to which extent a legal framework contributes to the control over the personal data.
Next, the legal constraints placed on or affecting the process will be assessed. This analysis segments the age groups and determines at which scale the

- conciseness,
- transparency,
- intelligibility,
- ease of access of information and
- language used in the scope of the privacy communication between organizations and users affect the legal control.

The limitation in this assessment is the assumption that the privacy modalities organizations communicate to individuals reflect the actual and truthful conditions within organizations. The factors listed above are derived from the GDPR, as it outlines the principles relating to processing of personal data in Art. 5. These principles must be defined in the scope of the documentation of processing activities, which in turn impact the quality and transparency of internal processes but also the level, depth and adequacy of information communicated to users.

Lastly, the legal control considers the effect of statutory requirements on IT systems and its effects on the user's ability to exercise control and improve trustworthiness. The measures include the effect of certification and verification mechanisms for lowering risk perception and improving trust [Kerkhof & Noort, 2010, p. 4]. Since the truthful conditions within organizations are not verifiable and the aim of this research is the conceptualization of a user-oriented online privacy control system, a substantial part of the analysis is placed on user perception (self-reported) rather than observed patterns, while later will be considered as well to some extent. The following analysis provides an in-depth definition for the corresponding user right presented in the subsequent table. The enforcement of these rights is coherent with compliance with the processing principles, defined in Art. 5 GDPR (Voigt & Bussche, 2017, p.150). Subsequently, Table 26 presents a holistic view on the scores provided by all respondents with regards to the importance of each data subject right. Irrespective of the age groups, the basic analysis reveals a ranking, distribution, and variance of preferences of each user right.
Overall, 70% of individuals are aware of their data subject rights. However, the subsequent assessment will further measure the level of confidence users have to exercise each right. Hereby, the assessment will focus on a crosstab analysis of “How important it is to exercise each user right” and “How confident are users are to exercise the user right”.
This assessment includes users with and without awareness of individual data subject rights. This decision is made, as the major concern is the effect of each right on the perception of control and trustworthiness as the crosstab results are equally important to understand from users that are not aware of such rights as users with existing awareness.

5.2. Conducting the experiment

The upcoming sections of the PhD dissertation focus on conducting the experiment from a legal perspective, including ethical and regulatory requirements. The aim is to provide a comprehensive understanding of the legal framework that governs the experiment and ensure compliance with legal and ethical standards.

A. Right to be Informed

The following points highlight the key takeaways for this user right, with respect to the impact on control and trustworthiness:

- access under Art. 12, 13 and 14 GDPR must take place proactively, as it presents an active obligation of the controller and processor;
- Art. 12 GDPR merely states the fact that controller and processor must transparently communicate privacy modalities for the exercise of the rights of the data subject;
- Art. 13 and 14 GDPR provide further guidance for controller and processor

respectively;

- provision of information must take place without undue delay but no later than one month and in case of complex and great number of requests (in proportion to the organization), the period may be extended by an additional two months, Art. 12 (3) GDPR;
    - the right to be informed considers any further request that a user places;
    - the right to be informed is associated with the right to data access (Voigt & Bussche, 2017, p.150) as they provide partial access, which is limited to the active information provisioning of an upcoming data processing activity. This is an example of the interconnectivity and mutual coherence of GDPR articles
    - this can further be the right to be informed about, e.g., if a rectification took place or a deletion request has been completed;
- requests must be provided free of charge

While almost 60% of respondents state that it is very important to be informed about their rights (see Table 26, appendix 3), only 23% are also confident and 28% very confident to exercise the respective right, or a cumulative 51% of all respondents, as the table below represents[22]. There is still a gap of almost 10 percentage points, which shows a residual uncertainty about the confidence. Although this user right is an active information obligation of organizations, individuals are not fully confident or might not fully trust organizations to meet this obligation.

Even if the two classes in the crosstab are aggregated together (highlighted in the table below in blue), merely 64% of respondents represent the upper two confidence classes. In comparison, 96% (see Table 26) of individuals are in the upper two confidence classes, irrespective of the user confidence level. The delta of 32 percentage points reflects that one in three individuals is still not or not fully confident to exercise a right that they perceive as important. The crosstab analysis clearly highlights the importance of drilling down into the data and identifying user preferences from different perspectives. This fundamental right can be seen as an elementary entry point to the observance and enhancement of all subsequent data subject rights.

[22] Observations here include comparing the importance of exercising rights against the importance of being informed.

Table 14: Crosstab of "Right to be informed"

General importance of the "Right to be informed"[a]	Confidence level to exercise the "Right to be informed"[b]				
	0	1	2	3	Don't know
0	1,3%	0,3%	1,3%	1,0%	0,0%
2	3,0%	6,6%	10,2%	12,1%	3,3%
3	4,6%	8,9%	23,0%	18,4%	6,2%

[a]Score values read as follows: 0 = not important at all, 1= less important, 2= important, 3 = very important. Score value 1 is left out due to insignificance of available data.
[b]Score values read as follows: 0 = not confident at all, 1= little confident, 2= confident, 3 = very confident.

B. Right to Access Data

The following points highlight the key takeaways for this user right, with respect to the impact on control and trustworthiness:

- according to Art. 15 GDPR, providing technical and organizational ways for individuals to access information on the scope, purpose and means of underlying processing activities and access to the data categories and inherent data processed by an organization;
- technical and organizational measures include features to drill down and receive further details into the personal data processed by an organization, to ensure in-depth data access possibility (Voigt & Bussche, 2017, p.150);
- data may be provided in "commonly used electronic formats", e.g., PDF or Word files, unless otherwise requested by the data subject, in acc. to Art. 15 (3) GDPR
- minimum information requirements are:
    - the purposes of the processing;
    - the categories of personal data concerned;
    - the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations;
    - where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
    - the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
    - the right to lodge a complaint with a supervisory authority;
    - where the personal data are not collected from the data subject, any available information as to their source;

- if applicable, information about the logic involved as well as the significance and the envisaged consequences of automated decision-making, including profiling for the data subject, referred to in Art. 22(1) and (4) GDPR
- information on data transfers to third countries (countries outside the EU or EEA, where the GDPR is not applicable)

The preceding list of access rights shows the enhanced privileges users receive through the GDPR. However, these legal foundations must be "baked" or integrated into the existing workflows. Other than the right to be informed, an access request must take place from the user (Voigt & Bussche, 2017, p.150). The request must include explicit details on the personal data, i.e., a mere confirmation of the data is not sufficient.
The table below depicts the crosstab of responses with regards to the importance level and confidence to exercise the access right. 60% perceive this right as very important. However, looking at the data column-wise, there is a tendency that individuals' confidence is more widely distributed. Therefore, it can be concluded that, although users perceive this right as very important, the confidence to exercise is not on the same level with the importance. Overall, the right to access has the highest concentration of responses across all categories (see Table 26). The delta here is almost 40%, compared to the 58% sum of the upper two crosstab classes and the 98%, in accordance with Table 26. Therefore, the design of the privacy control system should prioritize the development of features to enhance this privacy right.
The basis for this is provided by Art. 15 in association with Recital 63 GDPR; data is to be made available in electronic form, where possible through an interface as this helps to simplify access to the data. In this way, the GDPR provides a strong framework (1) to protect the user and (2) to further increase control over the data.

Table 15: Crosstab of "Right to data access"

General importance of the "Right to data access"[a]	Confidence level to exercise the "Right to data access"[b]				
	0	1	2	3	Don't know
0	0,4%	0,0%	0,4%	1,1%	0,0%
2	0,4%	4,0%	9,7%	9,7%	0,0%
3	0,4%	11,9%	29,6%	28,5%	4,0%

[a]Score values read as follows: 0 = not important at all, 1= less important, 2= important, 3 = very important. Score value 1 is left out due to insignificance of available data.
[b]Score values read as follows: 0 = not confident at all, 1= little confident, 2= confident, 3 = very confident.

A possible limitation of the right to access is that organizations shall only provide information which is directly obtained or generated by individuals. Subsequently, any insights produced

by organizations must not be shared. Otherwise, this right could be used to enforce the disclosure of corporate secrets, which could have adverse effects on the competitiveness of corporations (Voigt & Bussche, 2017, p.153). Furthermore, if large quantities of information are processed by an organization, the user must explicitly ask for the specific data he/she desires, otherwise a non-specific request can be rejected (Voigt & Bussche, 2017, p.152).

C. Right to Data Rectification

According to Art. 16 GDPR, where incorrect or incomplete data (Voigt & Bussche, 2017, p.154) prevails, or where the data does not reflect truthful information, individuals can obtain from the controller the correction, i.e., rectification of personal data. The right to rectify is a great medium to exercise control but also improve data integrity and thus trustworthiness. Incorrect, inaccurate, or incomplete data, which cannot be rectified could have negative effects on individuals. Considering only the rating level "very important", the right to rectification reaches the highest score across all subject rights, according to the survey (see Table 26). In comparison, the crosstab below (Table 16) shows that 64% perceive this right as very important, while a greater distribution in the actual confidence level persists. The deviation, reflected in the distribution of the importance and confidence levels, highlights a residual dissatisfaction about existing frameworks or channels for users to exercise their right.

Table 16: Crosstab of "Right to rectification"

General importance of the "Right to rectification"[a]	Confidence level to exercise the "Right to rectification"[b]				
	0	1	2	3	Don't know
0	0,3%	0,3%	0,3%	0,3%	0,0%
1	0,7%	2,0%	2,4%	1,4%	0,0%
2	0,0%	1,7%	2,0%	2,7%	0,0%
3	2,4%	16,7%	36,4%	27,9%	2,4%

[a]Score values read as follows: 0 = not important at all, 1= less important, 2= important, 3 = very important. Score value 1 is left out due to insignificance of available data.
[b]Score values read as follows: 0 = not confident at all, 1= little confident, 2= confident, 3 = very confident.

This user right is strongly associated with the right to erasure, according to Article 19 and Recital 65 GDPR. In this context, where the retention and thus the legitimacy for the processing of such data ends, data must be erased, i.e., through a rectification in data processing systems. Due to the chance of high correlation of both rights and thus, effects on control and trustworthiness, an interim summary will identify and discuss the effects on the conceptualization of the user control system.

D. Right to Data Erasure

The following points highlight the key takeaways for the right to erasure, with respect to the impact on control and trustworthiness:

- under Art. 17, further defined in Art. 5 (1) lit. C in relation to the purposes for which the data was processed, data must be deleted in the sense of the data minimization principle, i.e., limited to what is necessary in relation to the purposes for which they are processed. Consequently, if the data is no longer needed, it must be removed.
- deletion must take place in any downstream processings, i.e., in systems of the controller and processors, incl. backups (Alford, 2020, pp. 209-210). Where the deletion may be technically too complex, e.g., deletion in backups, a backup retention schema must be integrated that ensures deletion at a specified date.
- rejection of a deletion request can happen in the case of (1) complex and great number of requests and (2) juristidical (e.g., ongoing investigations) or statutory obligations (e.g., tax act). In either case, the organization needs to justify its decision and thoroughly document the facts that lead to the respective assessment (Ustaran, 2019, pp. 78-79) as well as communicate the decision to the affected individual.

Although the rejection of a deletion request limits users' ability for data control, the regulation prevents the GDPR from being used to conceal evidence, e.g., in case of criminal investigations. A cumulative 85% of users rated right as the third highest in terms of the level of importance, whereas the sum reflects the responses of important to very important.
The cross tab below reveals a wider distribution in terms of the confidence levels. Roughly 36% are either not confident at all or very little confident that they can exercise this right, irrespective of the general perception of the importance of this user right. Further, 12% of individuals seem to not perceive this right as important at all.
The intuitions of users reflect the challenges that organizations frequently address when it comes to the deletion of personal data from downstream systems. This causes a technical inability to fully comply with GDPR requirements. It can therefore be anticipated that a substantial number of organizations process such requests on a manual ad hoc basis rather than having an automated process in place.

Table 17: Crosstab of "Right to Erasure"

General importance of the "Right to erasure"[a]	Confidence level to exercise the "Right to erasure"[b]				
	0	1	2	3	Don't know
0	1,5%	2,2%	3,7%	3,7%	1,1%
1	1,5%	0,4%	0,7%	0,4%	0,0%
2	0,7%	1,5%	2,2%	2,2%	0,4%
3	10,7%	17,3%	20,2%	23,5%	6,3%

[a]Score values read as follows: 0 = not important at all, 1= less important, 2= important, 3 = very important. Score value 1 is left out due to insignificance of available data.
[b]Score values read as follows: 0 = not confident at all, 1= little confident, 2= confident, 3 = very confident.

Since the right to erasure strongly depends on other legislations, such as tax laws, which require the retention (storage) of personal data for such purposes, the level of confidence may be affected by that. This circumstance immediately affects the level of control over the data as it is limited by statutory obligations organizations are restricted to comply with.
Moreover, due to the burden of proof (Voigt & Bussche, 2017, p.159) individuals must provide evidence for the right to erase data. Implementing technical and organizational measures that record and map all personal data across various systems increases the transparency over data flows while further allowing organizations to meet the deletion requests of users. This would further automate the integration of such procedures into the privacy control system.
The identified technical and organizational complexities reflect the burdens for organizations to meet their obligation. This matches user perception, in terms of importance and confidence for exercising this right.

E. Right to Restrict Processing

The following points highlight the key takeaways for this user right, with respect to the impact on control and trustworthiness:

- according to Art. 18 GDPR sets forth criteria for restricting the processing of personal information:
    - the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
    - the processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
    - the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment,

exercise or defense of legal claims;
    - the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject;
- This right may be understood as a temporary measure (Ustaran, 2019, p. 80) for users to enforce their right, for as long as preceding circumstances prevail.

Table 18: Crosstab of "Right to restrict processing"

General importance of the "Right to restrict processing"[a]	Confidence level to exercise the "Right to restrict processing"[b]				
	0	1	2	3	Don't know
0	1,7%	1,7%	0,7%	2,0%	0,7%
1	3,4%	6,1%	0,7%	3,1%	1,0%
2	2,0%	5,1%	1,0%	2,7%	0,3%
3	10,5%	22,4%	8,2%	23,5%	3,1%

[a]Score values read as follows: 0 = not important at all, 1= less important, 2= important, 3 = very important. Score value 1 is left out due to insignificance of available data.
[b]Score values read as follows: 0 = not confident at all, 1= little confident, 2= confident, 3 = very confident.

According to the responses, this right is overall rated among the less important ones and has the highest distribution. Considering the criteria stated above for exercising this law, it can be concluded that the right plays a more subordinate role than other users' rights. This means for the design of the functionalities of the control system that it can be placed rather below the higher rated user rights features.

F. Right to Data Portability

The following points highlight the key takeaways for this user right, with respect to the impact on control and trustworthiness:

- essentially moving or transferring personal information from IT systems of one organization to another organization;
- Art. 20 GDPR explicitly focusses on strengthening the users control over data, through the minimization of the customer lock-in effect;
- data may be provided in "commonly used electronic formats", e.g. XML or JSON file – a PDF is not sufficient, as the transfering is considered as more complex, due to the limited compatibility of various IT systems;
- limitation: the portable data is limited to what the user has provided to the

organization (Voigt & Bussche, 2017, pp.170-171).

Table 19: Crosstab of "Right to data portability"

General importance of the "Right to data portability"[a]	Confidence level to exercise the "Right to data portability"[b]				
	0	1	2	3	Don't know
0	1,1%	1,8%	4,3%	1,8%	1,4%
1	0,7%	2,2%	1,8%	0,7%	0,4%
2	3,9%	9,7%	11,5%	9,3%	2,5%
3	3,6%	12,2%	14,3%	10,8%	6,1%

[a]Score values read as follows: 0 = not important at all, 1 = less important, 2 = important, 3 = very important. Score value 1 is left out due to insignificance of available data.
[b]Score values read as follows: 0 = not confident at all, 1 = little confident, 2 = confident, 3 = very confident.

Interestingly, the right to data portability has the lowest importance rating, considering the highest achievable points. Roughly 45% of all respondents state that this right is very important to them. From a privacy point of view, this right enhances the user right dramatically, as it prevents a lock-in effect.
User rights are strengthened through the control over their data by legally empowering them to change providers anytime (Voigt & Bussche, 2017, pp.168-169). Recital 68 of the GDPR specifies details on the rights of users and requirements for organizations to adhere to the law and thus ensure users to exercise their rights effectively:

> To further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller. Data controllers should be encouraged to develop interoperable formats that enable data portability. That right should apply where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract.

The recital highlights four important aspects for the data portability:

1. Processing carried out by automated means:
    a. In accordance with Art. 2 and in association with Recital 15 GDPR, processing of personal data, which form partly or wholly a filing system, can take place by machines or manually. Thus, Recital 68 is only applicable to processing activities where the processing takes place by machines, i.e., by automated means.

   b. Although the GDPR is technology neutral, i.e., the laws apply equally to manual and automated processing, the term "automated means" is clearly distinguished from manual means according to the Convention for the Protection of Individuals regarding Automatic Processing of Personal Data of the European Council (Council of Europe, 1981, pp.1-2). It is further elaborated in a definition provided by the European Commision (n.d.), differentiating automated from manual processing.
   c. A further indicator for automated processing is the provisioning of information, which must take place in a "commonly used, machine-readable and interoperable format", according to Recital 68 GDPR.
2. Right to portability may only be exercisable if the underlying legitimate basis is based on the user's consent or necessary for the performance of a contract. These grounds only represent ⅓ of all possible use cases. Other frequently used legal grounds, such as legitimate interest, are not affected. Consequently, the privacy control interface could provide such a service, which however, would be limited to the two identified legal bases. From a technical implementation perspective, an automated assessment in the background would need to take place. This, however, requires the organizations to fully map/provide the legal basis for all processing activities. A possible solution would be the set-up of a standardized Records of Processing Activities (RoPAs) framework, in accordance with Art. 30 GDPR. This would allow organizations to document all processes, while allowing users to exercise their rights.
3. The provisioning of structured, commonly used, machine-readable and interoperable formats:
   a. Based on the Eur-lex glossary (n.d.), which reflects laws and regulations of the Court of Justice of the European Union, the Article 29 Working Party (2016, pp.17-18) defines commonly used and machine-readable formats a.o., as XML, JSON and CSV.
   b. The term "interoperability" of Recital 68 GDPR shall further encourage organizations to mutually develop standard formats. This further shows the GDPRs encouragement for uniformity.

The user right could be exercised through the interface, by allowing users to request a transfer directly through the interface. The three-step approach in the Figures below depicts a possible process implementation.
Users select the organizations affected by the data transfer request. If an organization is not yet available, a login dialog for the web appears, which would require the integration of various software development kits (SDKs) – here exemplary displayed with Google, Apple, and Facebook.

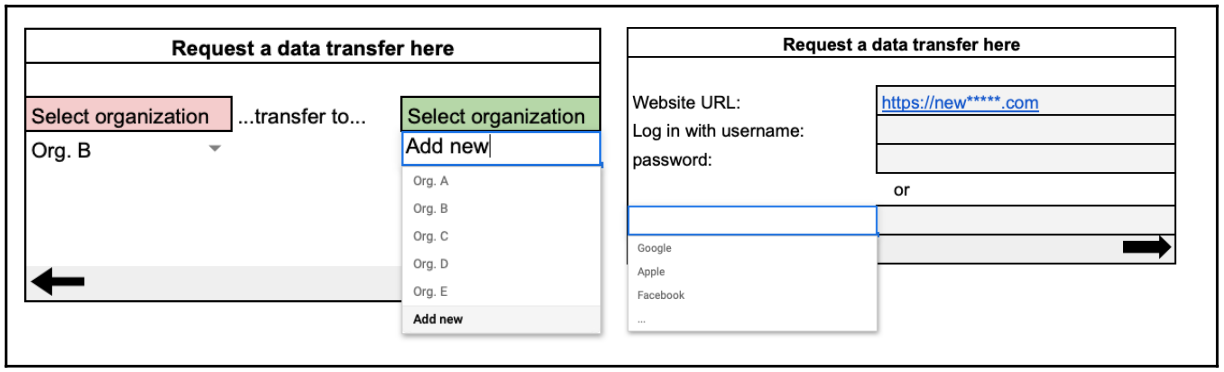

Figure 26: Mockup of Data Transfer Request (1)

A summary of information will be provided in case of successful data retrieval.

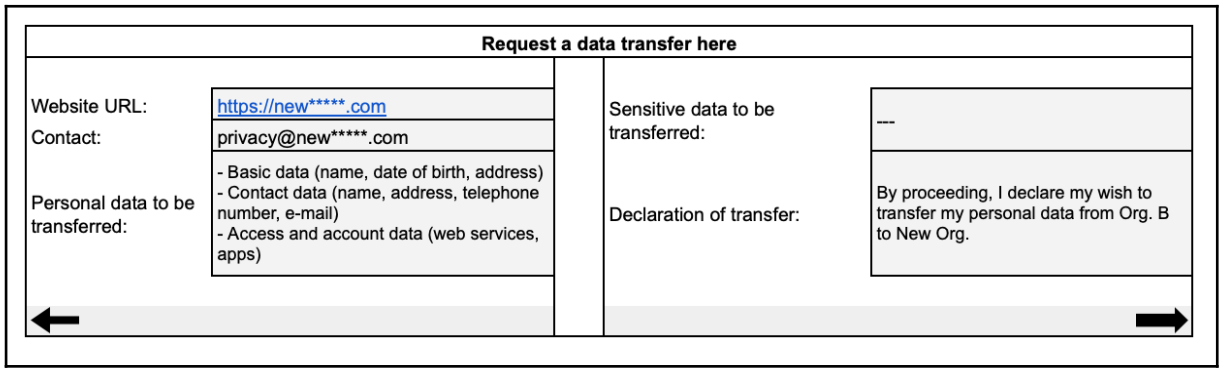

Figure 27: Mockup of Data Transfer Request (2)

The final transfer information will take place as presented below. In case of unsuccessful data retrieval, the right window below will provide further information and action.

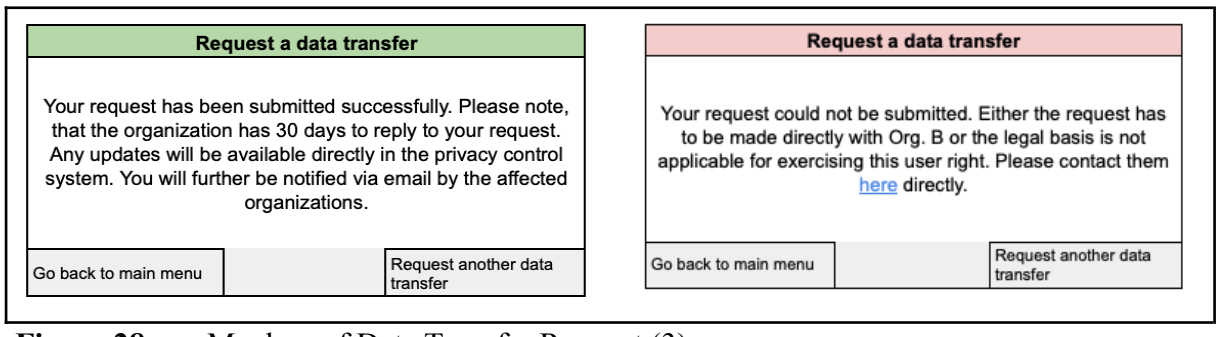

Figure 28: Mockup of Data Transfer Request (3)

In summary, the users intuitively identified that this user right is only applicable in ⅓ of all data processing activities carried out by organizations. Nevertheless, the detailed analysis of this user right identified the importance of implementing a system feature that enables users to transfer their data among different organizations. A potential proposal, see mockups above, provided a tangible layout structure for the implementation.

G. Right to Object to Data Processing

The following points highlight the key takeaways for this user right, with respect to the impact on control and trustworthiness. Art. 21 GDPR sets forth three scenarios, where users can object to the processing:

- first, if the processing, in association with Art. 6 (1) lit. e and lit. f GDPR, is based on legitimate interest and is carried out in the performance of a task in the public interest. The exception is, if the legitimacy for the processing overrides the interests, rights and freedoms of the data subject, according to 21 (1) GDPR;
- second, if the processing is associated with direct marketing purposes, i.e., marketing activities, where the user is directly targeted based on one or more characteristics or personal features that makes the individual targetable for specific campaigns;
- third, where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), according to 21 (6) GDPR.

Same as the right to data access and right to be informed, the right to object to data processing does not provide ratings for "less important".

Table 20: Crosstab of "Right to object to data processing"

General importance of the "Right to object to data processing"[a]	Confidence level to exercise the "Right to object to data processing"[b]				
	0	1	2	3	Don't know
0	1,1%	0,7%	2,5%	3,2%	1,8%
2	0,7%	1,4%	1,8%	1,8%	0,7%
3	4,6%	15,4%	16,8%	34,7%	13,0%

[a]Score values read as follows: 0 = not important at all, 1 = less important, 2 = important, 3 = very important. Score value 1 is left out due to insignificance of available data.
[b]Score values read as follows: 0 = not confident at all, 1 = little confident, 2 = confident, 3 = very confident.

H. Right to Object Automated Processing

The following points highlight the key takeaways for this user right, with respect to the impact on control and trustworthiness:

- Automated decision-making, including profiling, refers to any processing of personal data, where legal effects or consequences are the result of a data processing that does not involve the intervention or decision making of a human being, according to Art. 22

GDPR.

- Examples according to Recital 71 GDPR include the automatic refusal of an online credit application or e-recruiting practices without any human intervention.
- Organizations can implement a human decision step, often providing the final verdict, which bypasses this law. Nevertheless, organizations will not be exempt from any other GDPR regulation.
- Three exceptions, that enable lawful automated decision, according to Recital 71 GDPR, are:
    - that the user provides explicit consent,
    - that the processing is necessary for the entering or performance of a contract between the user and a controller,
    - that it is expressly authorized by Union or Member State law.
- These exceptions do not reflect limitations for the exercising of user control over their data, they rather add stricter guidelines for organizations to process the personal information and thus create a positive sum game.

Table 21: Crosstab of "Right to object to automated data processing"

General importance of the "Right to object automated processing"[a]	Confidence level to exercise the "Right to object automated processing"[b]				
	0	1	2	3	Don't know
0	0,3%	0,7%	2,4%	1,4%	0,7%
1	2,4%	3,7%	4,7%	5,8%	1,4%
2	1,7%	3,1%	5,1%	5,1%	1,7%
3	7,5%	12,2%	13,6%	16,6%	10,2%

[a]Score values read as follows: 0 = not important at all, 1 = less important, 2 = important, 3 = very important. Score value 1 is left out due to insignificance of available data.
[b]Score values read as follows: 0 = not confident at all, 1 = little confident, 2 = confident, 3 = very confident.

The assessment of importance and confidence to exercise each user right allows a ranking of such rights and leads to the specification of features for the control system. Higher rated rights, i.e., the right to object to data processing, right to rectification and right to data access must be placed more visibly and should be easily accessible for the users.
The data does not show any specific preferences for individual age groups, rather a homogeneous distribution is observable across all drill-down dimensions.
A separate study on benchmarking user perception and true organizational condition of IT systems would further contribute to transparency in the efforts to enhance trustworthiness and data control, but also improve compliance of organizations.

The largest obstacles organizations face have already been identified in chapter 1.4 “The Data Protection Compliance Dilemma” and can be used as a basis for future developments.

5.2.1. Technological Control over Data, Processes, and IT Systems

This chapter assesses to what extent users are enabled through technological features to exercise their control over data, processes, and IT systems. The analysis takes place across the dimensions of age group, occupation, and device usership, which involves an evaluation of nine crosstabs in total. Specifically, the analysis of survey responses will determine the level of confidentiality, integrity, and availability, i.e., reliability of data processing technologies and systems. The survey responses are all based on individuals' perceptions on the various subjects, thus reflecting the user's perspectives on these matters.
As identified in chapter 2.3 Definition of Trust and Trustworthiness, IT suspicion, although independent of trust and distrust (Lyons et al., 2011, p.224), correlates positively with greater engagement in information search, proportionally to the individuals with less suspicion. The findings of Lyons will be applied to this research and tested for the following conditions:

1. if conciseness, transparency, intelligibility, ease of information access and the language used in the privacy control system improve trustworthiness and decrease suspicion;
2. if users' perception of technological data control influences the level of trustworthiness;
3. if user suspicion towards IT systems affects trustworthiness.

The statements from above and corresponding answers are presented below.

1. If conciseness, transparency, intelligibility, ease of information access and the language used in the privacy control system improve trustworthiness and decrease suspicion

The assessment above highlights three of the most impactful control features segmented by highest rated user statements. These three elements call attention to the importance for users to affirm their confidence in exercising their rights and further decrease technology suspicion.
This finding is further strengthened by the results of the crosstab assessment of age groups and how the following features enhance the understanding of a privacy policy. The analysis is conducted for occupation and device userships as well and matches the results of the age groups. The user statements are as follows:

Table 22: Assessment of Most Statements for Impactful Control Features

Statement	Evaluation
detailed descriptions (the more details the better)	45% of survey respondents across various age groups prefer less details, which affirms the above identified results as well as the reference paper (Lyons et al., 2011, p.224)
structured headers and sections (collapsible text blocks)	52% prefer very structured headers and sections, incl. collapsible text blocks feature (including the next score value, i.e. 3 and 4, it is noticeable that almost 90% are in favor of this feature)
icons enhancing the policy	40% claim that icons would somewhat improve control over data, but in consideration of the entire data do not regard this feature as essential
videos explaining technical terms and usage of your data.	Similar to icons, it is observable that videos are somewhat improving the control. This is due to the passive nature of both icons and videos, as they only provide explanation of the underlying processing, whereas interactive header structures seem to increase the control perception. Hence, the user interface design and particularly the placement of features for easy access would cut time for information search and as a result decrease IT suspicion.

2. If users' perception of technological data control influences the level of trustworthiness

Across the age groups, users have been asked to rate how the following features would improve the trustworthiness of organizations:

a) confidential (secure, reliable) treatment of my data (through an org., system, etc.),
b) ensuring integrity: organizations keep their promises/honesty, act reliable with data,
c) making the handling of my data transparent and available at any time.

While the previous section shows how the privacy information should be presented, i.e., user interface and experience, this evaluation presents the means to achieve trustworthiness through the privacy design features as well as clear documentation on certain aspects presented above.
The survey participants were further asked “Please indicate to what extent each statement would give you control over your data after sharing it with organizations” and subsequently presented with nine statements with various score values.[23] The assessment of the crosstab shows that 67% of the age groups between the age of 20 and 45 rated all listed features above as very important. The evaluation of the other two dimensions (occupation, device usership) produces an identical picture. Data of the remaining age group are excluded due to insufficient number of responses for this crosstab. Following statements score the 3/3 points:

[23] Score values read as follows: 0 = not important at all, 1 = somewhat important, 3 = very important

- It makes me more confident to have control over my data, If organizations (internally) have strict data access policies,
- It is important that organizations always ensure that my data is accessible for me (e.g., via a user account),
- Control over my data is strongly connected to concise, transparent, intelligible, and easily accessible privacy information.

Survey participants further strongly disagree with the following statement:

- I prefer detailed (extensive) information on the technology used in an organization.

This question is affirming and confirming the exploration of features enhancing the understanding of privacy policy, but also testing the research results of the reference paper (Lyons et al., 2011, p.224), which can be positively confirmed. Indeed, it can be concluded that there is a link between lower IT suspicion and subsequent decreased efforts for information search, if the information is presented in a user-friendly manner. The main aspects that play an essential role are the three conditions that have been identified in the initial paragraph of this chapter, which have been tested against the reference paper results.
These findings are in complete contrast to what organizations have been doing with their privacy policies since the GDPR came into effect. Researchers have found that policy texts have increased in length and word count (Sobers, 2020). Thus, reading a policy start to end will take more than 10 minutes (Mcdonald & Cranor, 2008, p.554), a threshold that is more than twice as high, as an independent study conducted as part of this doctoral research shows.
Altogether, the research results can be condensed to a few essential requirements that have to be met to create trustworthiness for the end users on the one hand, but also allow those users to have the necessary control over their own data on the other hand. It is essential that neither an information overload nor too many functionalities are provided, but that they are presented selectively, through easy interface navigation and communicated in a simple language, according to the principle "less is more".

3. If user suspicion towards IT systems affects trustworthiness

The determination of the emotional background as well as the background knowledge of the survey participants aims at concluding a representative sample from the population with regards to an inherent level, resp. baseline for technology know-how. Following Lyons et al. (2011) experiment, this facilitates an understanding of how it affects the suspicion and trustworthiness towards technologies used in organizations. Consequently, it will not only be possible to measure the level of information needed to minimize suspicion and increase

trustworthiness and transparency, but also to find out how much of an information gap is acceptable to still reach a certain level of trust.
Survey participants have been asked to what extent certain features and information provided on technology would reduce their suspicion and help understand the technologies that companies use to process data. The three most frequently selected and highest rated answers – ordered by the average ratings – are:

Table 23: Average Consensus Rates of Top Statements on Reduction of IT Suspicion

Statement	Rating
use of plain language (of all information provided to you)	74%
ease of information access (e.g. easy navigation and identification of specific privacy topics)	68%
transparency of data processing (What does the technology do with my data?)	66%

These results further strengthen the preceding analysis findings. While the underlying IT system is relevant to users, there is a stronger need for the use of plain language, ease of information access and transparency of data processing technologies. Similar to the requirements for the better comprehension of a privacy policy, the reliability of data processing technology starts with the provisioning of documentation of such technologies for users.
It is important to recognize that all requirements are mutually reinforcing, i.e., each building block improves the entire trustworthiness as well as control mechanism rather than solving a niche requirement of the privacy framework.
In order to solidify these findings an additional verifying statement was provided to the participants and goes as follows: “If the organization is accredited with certifications of official bodies (e.g., EDPS, ICO, ISO, NIST), it would lower my risk perception towards technologies used in an organization”. This is plotted on the x-axis in the Figure below, on a scale from 0% to 100%, whereas the former percentage stands for “strongly disagree” and the latter means “strongly agree” with a mean response rate of 72%. A segmentation into three sections (disagree, agree or neutral) further reveals a tendency to a left-skewed distribution. A pronounced distribution of the data scatters in the range of the mean value, which is allocated in the third zone. This is important to consider, as it provides the bigger picture of response behaviors. Excluding neutral responses, merely 13% are in the first zone, i.e., disagree, whereas 88% are in the third zone, i.e., agree. Consequently, the majority of individuals acknowledge that certifications of organizations have a positive impact on the improvement of trust.

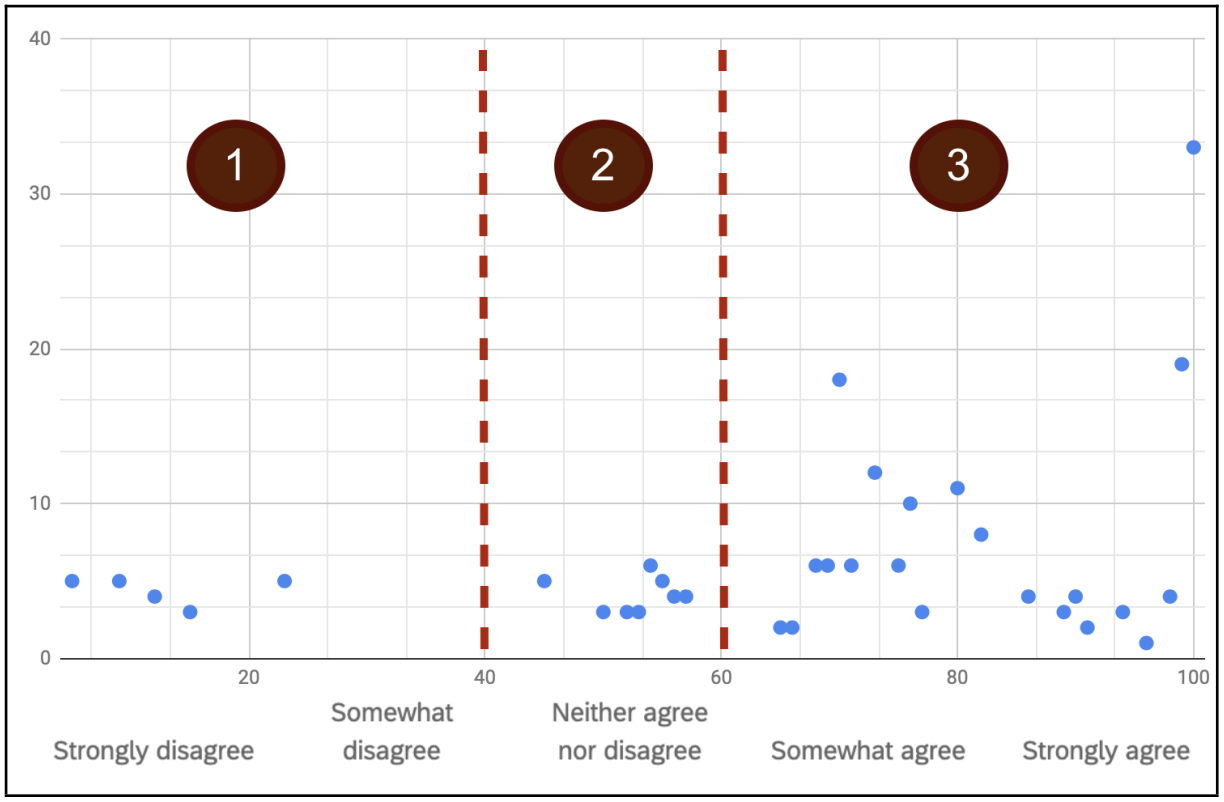

Figure 29: Effects of Certifications on the Trustworthiness of Organizations

A second crosstab assessment with the question "Does it matter if you know the certificates that the company was awarded?" reveals deeper insights on the response behavior of survey participants.

On a slide bar from 0% to 100% (equivalent to "strongly disagree" and "strongly agree") almost ⅓ of all responses strongly agree with the statement (greater or equal to 90%). An isolated view on the remaining ⅔ shows an average towards the 70% "agree" mark.

The crosstab highlights the importance of certifications for the benefit of trust towards organizations. It can therefore be concluded that such certifications act as an effective measure for minimizing user suspicion towards IT systems and consequently improve trustworthiness.

Limitations to the analysis of technological control are the constraints to the objectification of the security of processing (Art. 32 GDPR) and the 14 security requirements provided in section 64 BDSG. Such analysis is only objectifiable for a full reflection of the actual state of such controls through an organizational assessment. They cover and directly impact trustworthiness on processes and IT systems and strongly depend on organizational internal setups. Since this research is limited to the objectification of end user perceptions of these elements, the research results, particularly of the importance of certifications for building trustworthiness, highlight the importance of user-friendly privacy by design elements in the control system. Hence, an assessment of security elements from an organizational perspective,

e.g., in the scope of an audit or certification process, would strengthen the credibility of organizational compliance with the above stated laws.

5.3. Conclusion

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 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. Thus, in the scope of this chapter, the underlying data underwent a descriptive assessment and was analyzed in detail that included an exploration of relationships between the responses. Subsequently, the responses were analyzed isolated for each question and in a crosstab assessment manner. To facilitate a systematic analysis, a three-dimensional framework (cube) was designed for the analysis of trustworthiness building factors based on the insights resulting from the assessment of relevant research papers as well as the conduction of preliminary surveys. The analysis included a descriptive data analysis and a subsequently segmented analysis of control perceptions over data, processes, and IT systems from a psychological, legal, and technological view. The results of all assessments revealed that there is a homogeneity in the responses within each and across all segments (age group, occupation, device usership). Consequently, it is suggested that the observed patterns of individuals' behavior can be analyzed to draw broad conclusions about the data without segmentation. Yet using detailed segmentation seems necessary for more detailed statements.

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[24].
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 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.
To create a tangible and measurable level of abstraction for the three preceding attributes, the emotional and domain specific background, i.e., level of privacy understanding of the survey participants was evaluated. This approach facilitates a more precise definition of the content of privacy modalities as well as the user interface design to ensure the best possible user experience, which ultimately contributes to the increase in trustworthiness.
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

[24] See Figure 16 for details, color scale used to highlight users' active power to exercise control over their data

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.

5.4. Results analysis

5.4.1. Summary of Research Findings for the Personal Privacy Cockpit (PPC)

This chapter summarizes the identified modules and specifications of the online privacy control system. The following synopsis provides a concise overview of the system modules and insights gathered from the preceding analysis. It further discusses each element's feasibility and effectiveness for the increase of control and trustworthiness and finally provides a conclusion on its operationalizability and complexity reduction.

5.4.2. Requirements Specification of System Modules

The modules for the control system have been derived from the privacy cube (see figure 16, 3D concept of trustworthiness building factors). 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 (see figure 25) 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. The summary findings in table 24 (table elements 4, 5, 6) list out the explicit features. Processes (a) and underlying technologies (IT systems (b)) are set up on top of the legal framework. In consideration of the nature of business operations they determine the processing (usage), retention and deletion of the data (c). A, B and C in total represent the organization (x-axis).
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[25] 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. The simplified workflow below summarizes this:

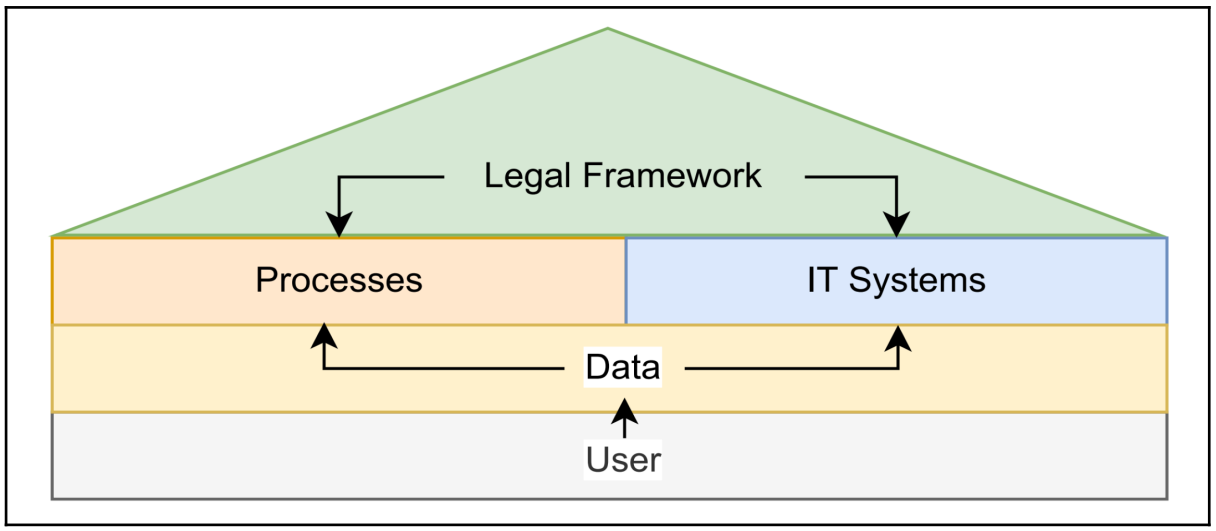

Figure 30: Simplified Composition of Relevant Subject Matter Symbiosis

[25] Organization comprises the data, processes and IT systems in figure 30.

5.4.3. Summary of System Modules Analysis

In order to provide a systematic approach for the summary of the system module specifications, a corresponding table (table 24) is provided at first. The numbered fields are in line with the subsequent paragraphs, which conclude the findings achieved throughout the research.

Table 24: Corresponding Table for System Modules Requirements

		Organization		
		Data	Processes	IT systems
Control	Psychological	1.	2.	3.
	Legal	4.	5.	6.
	Technological	7.	8.	9.

Corresponding summary of findings below:

1. Summary of “Psychological Control” and “Data” Crosstab Findings Below

The analysis of the psychological control over data first involved data segmentation in accordance with the key measurement indicators (table 5). It has been identified that most information is exchanged by the age groups 26 to 35, with data typically passed once a week or rarely.
Users across all age groups tend to be more comfortable sharing non-sensitive data while being more inherently conservative in sharing sensitive information, showing an alignment with the GDPR in terms of the differentiation between non-sensitive and sensitive personal identifiers. Information that is perceived as less sensitive tends to be more frequently shared, or there is a higher degree of openness to share such data and vice versa. Location data (GPS data, etc.) and web data (website visits, clicks, posts, likes, comments, cookies, etc.) are most frequently shared, accounting for roughly 25% of all data types presented in the survey.
The second assessment stage reveals insights into user attitudes and thus psychological perceptions about data control. The identification of the types of personal identifiers, their sharing frequency and how users perceive their data, i.e., non-sensitive or particularly sensitive, allowed the measurement of the actual handling of their own data. In addition, it was found that users tend to have a low level of basic trust in organizations, which was derived from the increased information seeking. However, respondents also said that privacy information was not easy to find and was also difficult to understand. The latter two factors mean that despite users' awareness of their own data handling, their psychological perception of data control is limited.

Moreover, a paradigm shift can be observed in the trust that data subjects place in internet service providers with regards to data sharing. Users show an increased tendency towards the limitation of sharing personal information by updating privacy settings, limiting cookie tracking and making use of other technical measures. Concurrently, due to the complexity and variety of privacy interfaces as well as the lack of organizational compliance, users' ability to fully exercise their rights is limited.
The majority of individuals not originating from the EU are engaging with such practices for more than three years, driven by an increased concern about the data processing activities of corporations. However, the EU respondents state that the shift towards restrictive data sharing took place within the past two years. The entry into force of the GDPR in 2018 may have had a causal effect on user awareness. The interim conclusion shows that the increasing complexity and obscurity of provided data protection information affects user behavior towards limiting data sharing, while increasing the need for the development of user-centric privacy management solutions.
Lastly, survey participants regard blue as the most trustworthy building color. Based on the associative learning theory, blue is associated with peaceful and calm objects.
In addition, the introduction of green into the privacy control interface could lower suspicion of IT systems, thereby improving the perceived level of trustworthiness. Links to fan pages have proven to not have significant and meaningful effects on the establishment of organizations' trustworthiness.

2. Summary of “Psychological Control” and “Processes” Crosstab Findings Below

The evaluation was based on the criteria of conciseness, transparency, understandability, and ease of access to information as well as the language used to explain the processing. Specifically, accessibility of information, transparency of data processing and use of plain language are critical components for achieving trustworthiness, followed by clear disclosure of privacy interests and an effective risk mitigation process. Paper printouts, URL links, or QR codes for privacy modalities are all options for data collection from devices without screens to enhance a comprehensive, integrated and user-oriented data protection management. Ease of information access should be understood as (1) ease of navigation through the website to access privacy policies and (2) reducing the complexity of the privacy policies presented.
Looking at this from the user's perspective, it is certain that providing data access services or features and keeping the language simple would equally improve psychological control perception as well as increase control and trustworthiness. Transparency of processing activities is determined as just-in-time notification, inclusion of layered methods, but not just nesting of subpages.
There is a strong dichotomy between users' self-reportedly observed time spent reading a privacy policy and estimation of time needed to fully read a policy. Latter case is used as an

approximate substitute for the actual observation and measurement of time spent reading the policy. Users should be able to drill down into the information using privacy features that reduce the time spent searching for information and provide key privacy features in an easy-to-understand format. There needs to be an underlying process in place to ensure easy access to information about web data use, as this data is affected by breaches, is shared among users and is more sensitive than other personal identifiers.

3. Summary of “Psychological Control” and “IT Systems” Crosstab Findings Below

The data evaluation shows that (psychological) controllability of system features, i.e., the perception of being able to be equipped with the physical (or digital) means to exercise influence over an IT system that processes personal information, indicates the user's demand for functional requirements to achieve control over their data. Improved features increase engagement with privacy systems, leading to more included privacy content and better understanding. Access to the most commonly used personal data via IT systems is improved through ease of access and understanding of technical and organizational security measures. Respondents across all age groups prefer less detail, but instead highly structured headings and sections, including a collapsible text block feature. This feature can further be optimized by limiting the length of a privacy policy and thus the time it takes to read it. Moreover, the degree of personalization of system features indicates maintaining association with the corporate brand (colors, fonts, and logos) and embedding it in the privacy control system to facilitate organizational recognition and promote such integration into the control system.
Icons and videos are not as essential as perceived features to enhance the policy and explain technical terms and data use.

4. Summary of “Legal Control” and “Data” Crosstab Findings Below

The conclusions for this cross-tabulation are such that confidence in the exercise of user rights is limited, as respondents state that organizations may not meet their active information obligation, e.g., provide privacy notices when needed and in an adequate manner. Effectively, achieving legal control over the data means that organizations must offer such information on an upcoming personal data processing activity in a timely manner, in accordance with Art. 12, 13 and 14 GDPR. Other user rights, such as the ones under Art. 15 and 16, must further be offered through an interface. The interface must provide a feature that enables individuals to particularly exercise their rights of rectification, erasure, and objection to data processing in an easy way as presented in the mockups in figure 26-28.

5. Summary of “Legal Control” and “Processes” Crosstab Findings Below

Due to the limited degree of regulatory compliance of a considerable number of companies, a subsequent discrepancy of privacy policies and the actual processing activities that take place within the organization may be greater. Thus, when describing IT systems, conciseness, transparency, comprehensibility, easy access to information and clear language must be used. Consequently, the privacy control system should provide categories of data and provide detailed information about the underlying processing and (enhanced) security measures to protect them. The privacy information function or section (e.g., privacy notice) should include information about the controller(s) and processor(s), territorial applicability, the organization's data processing policies, purposes of data collection, categories of personal data, the relevant legal basis, profiling commitments and specifications for international data transfers.
Essentially, the legal control over processes is achievable through the provisioning of a privacy policy compliant with the foregoing requirements. The improvement of control over data is reflected in the comprehensiveness of credible privacy modalities provided by organizations to users. The lack of such leads to a decrease in legal control on both ends, i.e., users and organizations alike, while negatively affecting trustworthiness.

6. Summary of “Legal Control” and “IT Systems” Crosstab Findings Below

The effects of certification and verification mechanisms have been analyzed to identify their impact on the reduction of risk perception and improvement of compliance. Certifications (e.g., EDPS, ICO, ISO, and NIST) are effective means for reducing user distrust of IT systems and thereby improving trustworthiness.
Since actual organizational conditions cannot be verified, certification and verification mechanisms for IT systems that support processes and data handling help reduce risk perception and improve trust. Essentially, it is critical that users are familiar with the certifications, as this has a positive impact on the claims that the accreditation states. Links (icons) to the organization's fan page, such as Facebook, Twitter and Instagram have no meaningful effect, as it is perceived as less important across all segments.

7. Summary of “Technological Control” and “Data” Crosstab Findings Below

This assessment of the technological control over data identified the importance of confidentiality and integrity of data processing technology. Technological control over data is obtainable by users through easy access to their information, transparency of data processing technology and usage of plain language. Confidentiality and integrity is therefore not only achieved through the restriction, unauthorized access and alteration of data but through the strengthening of users' access control. Thus, two concurrent requirements are to be implemented to achieve technological control, which are the information and enabling active user intervention in the processing of their personal data. As with the requirements for a better understanding of privacy policies, the reliability of data processing technology begins with

providing users with documentation of such technology and its applicable usage. Optionally, the following three sections (1) Healthcare, (2) Social Media and (3) Finance and Insurance can be implemented to decrease the level of granularity and improve navigation through thematically coherent data processing organizations. Ultimately, control of data access is the authority of the individual user, not the access control of an organization.
From the user's perspective, the provisioning of data access self-service capabilities as well as maintaining understandable language will increase the control and trustworthiness alike.

8. Summary of “Technological Control” and “Processes” Crosstab Findings Below

This assessment identified that the critical factor for achieving technological control over processes is coherent with the time spent reading and understanding an organization's privacy policy. A strong discrepancy was found between the self-reported time users spend reading the privacy policy and the estimated time it takes them to read the entire policy. An introduction of privacy policy design features that reduce the need to search for information and allow users to dig deeper into the information, while condensing the most important privacy terms that are easy to understand are elements to improve control.
Thus, technological control refers to the users' understanding of the underlying processing activities and is highly dependent in particular on the ease of access to information, the transparency of data processing, the use of particularly simple language as an important feature to achieve reliability, the conciseness of data protection information and its comprehensibility.
Information accessibility means (1) making the website easy to navigate to access the privacy notice and (2) reducing the complexity of the privacy notice presented. It is less referred to as the provisioning of technical measures to enable users to control their data as this aspect has been fully elaborated in the preceding section 7.
It is further notable that in case of data collection taking place from devices without screens, the provisioning via paper printout, URL link or QR code, or a combination of various methods is crucial to improve the technological control over processes. To further increase the overall processing transparency, just-in-time notifications and layered method integration seem to be a necessity from a user perspective and thus, should be implemented, while avoiding mere nesting of subpages.

9. Summary of “Technological Control” and “IT Systems” Crosstab Findings Below

Technological control over IT systems is expressed through the crosstab legal and IT systems, particularly through the credibility, availability, and reliability of data processing systems. This crosstab is the least controllable module in the research framework[26]. It is characterized by the highest degree of intransparency, due to the nature of this crosstab combination, which

[26] see Figure 17 for reference.

limits the extraction capabilities of insights about organizations. In the course of the analysis a linkage between this crosstab and the preceding summary (point 6.) “legal control” and “IT systems” has been identified.
Based on this association, it was concluded that particularly the certification and verification of organizations seem to improve users' control perception over organizational IT systems and thus enhance trustworthiness. Hence, listing security measures does not enhance the users' ability to actively exercise control but increases transparency over organizational credibility, availability, and reliability measures. As a result of the improved clarity, which is further supported through certification mechanisms, organizational trustworthiness is positively impacted.

5.4.4. Conclusion of Online Privacy Control System Components

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 foregoing 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).

5.4.5. Critical Appraisal

The comparison of the adaptation probabilities of the peer privacy systems (see figure 5) 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 or even reducing 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 critical appraisal 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.

5.5. Conclusion

5.5.1. Evaluation of Control and Trustworthiness Through Privacy Control System

The aim of the dissertation was the definition of an operationalizable roadmap for the conceptualization of a user-centric privacy control system. This included the identification and analysis of critical functional and technology features, the theoretical design of a privacy control framework as well as the evaluation of user control over privacy features and effects towards corporate trust. Additionally, the system had to be GDPR-compliant, pragmatic, scalable and cross-industry-applicable. In order to facilitate a constructive evaluation of control and trustworthiness, the mutual effects of such have been analyzed. It has been concluded that control over personal data via a privacy control system establishes and enhances organizational trustworthiness. Hence, control can be regarded as a foundation or an entry point for creating trustworthiness. The analysis was conducted by systematically assessing the three main areas, i.e., the legal, technical, and psychological control spectrum.

The reasons for the decision to analyze the control from these perspectives were threefold: firstly, the fuzzy regulations and the lack of practical guidance for organizations to create compliant privacy systems for the data subjects, secondly, the existing technological burden and associated lack of resources to operationalize legal (GDPR) requirements in an effective manner and lastly uncovering the lack of user-centricity in present privacy solutions across industries. Thus, during the dissertation the legal assessment not only provided legal 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[27]. 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. Consequently, implementing the identified features will meet user behavior and improve engagement. Such measures would further decrease the attitude versus behavior dichotomy. 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.

[27] 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.

6. Dissertation Contributions

6.1. Scientific Research Contribution

The principal scientific research contribution of the doctoral thesis was the proposal of a comprehensive framework for ensuring GDPR compliance, which has yielded the following tangible outcomes:

- Proposed a framework for examining GDPR regulations in the context of connected medical technologies, which emphasizes the need for a user-centric privacy control system.
- Identified essential components necessary for the lawful and responsible processing of personal data in this specific domain, by applying the proposed framework.
- Validated the proposed framework by designing and implementing a questionnaire to collect and analyze data that can be utilized for future research in this domain.
- Developed an operationalizable roadmap for the user-centric privacy control system, by systematically assessing the legal, technical, and psychological control spectrum.
- Implemented privacy-by-design guidelines at both the operational and information system level to enable individuals to exercise their legal rights effectively and organizations to comply with GDPR requirements.
- Analyzed the mutual effects of control and trustworthiness, which revealed that a simple user-friendly interface was critical to control perception and organizational trustworthiness.
- Created a foundation for organizations to enhance their trustworthiness and achieve GDPR compliance by emphasizing the need for a user-centric privacy control system in connected medical technologies.

6.2. Scientific Publications

The scientific research contributions have been reported in relevant scientific journals and presented at scientific conferences. The following publications have already been completed and published in conference proceedings:

1. Assessment of the quality of user awareness of GDPR in healthcare IOT (Kadir Ider), published conference paper at BIA-2021 (International Conference on Biomedical Innovations and Applications),
2. Secure Public WiFi durch Network Access Control – Ansätze, Chancen und datenschutz-rechtliche Implikationen – May 2021 (published at the conference “Nachwuchswissenschaftler*innenkonferenz 2020/21” at EAH Jena),

3. DSGVO Compliance und Datenschutz-Managementsystem als Erfolgsfaktor für die Digitale Transformation nutzen (co-written, Kadir Ider and Prof. Dr. Michael Faustino-Bauer), published article in ZRFC Risk, Fraud & Compliance Magazine in Dec. 2020,
4. Data Privacy For AI Fraud Detection Models – A framework for GDPR compliant AI (co-written and peer-reviewed, Kadir Ider and Prof. Dr. Andreas Schmietendorf), published conference paper in The Fourteenth International Conference on Digital Society ICDS 2020 in Oct. 2020,
5. Effective Privacy Management Concepts: Increasing Privacy Control by Reducing Complexity (Kadir Ider), published conference paper in the 2020 Evaluation of Service-APIs (ESAPI) of the Central Europe Computer Measurement Group (ceCMG), published in Shaker Verlag GmbH in Oct. 2020,
6. Barriers for the Utilization of Open Data (Kadir Ider), conference paper in the 2019 Evaluation of Service-APIs (ESAPI) of the Central Europe Computer Measurement Group (ceCMG) in cooperation with Hochschule für Technik und Wirtschaft Dresden in Sep. 2019.

These publications demonstrate the significance and impact of the research contributions made in the current doctoral study. They also highlight the potential for future research in improving online privacy control systems and organizational trustworthiness.

6.3. Recommendation for Further Research

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 resp. 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.

7. Literature

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.

8. Appendice

Appendix 1 – Occupation and Age Group Matrix, Absolute Numbers

Table 25: Heat Map Segmentation of Occupation by Age Groups

	Age Group							
Occupation	20 - 25	26 - 30	31 - 35	36 - 40	40 - 45	46 - 50	51 - 55	Grand Total
Information Technology	12	39	27	19	8		1	106
Marketing, Sales and Service	9	40	35	10	7	1		102
Science, Technology, Engineering and Mathematics	4	31	33	8	9	1	4	90
Business Management and Administration	3	22	22	7	3		3	60
Finance	5	13	13	9	3			43
Law, Data Protection	1	8	8	4	4		1	26
Education and Training		1	1	2				4
Grand Total	34	154	139	59	34	2	9	431

Appendix 2 – Data Categories and Sharing Behavior Clustered by Age Group

The colored percentages reflect the proportionate distribution of responses per question for each data category, i.e., per row. A total number of absolute answers is provided in the "Total" column.

Table 26: Segmentation of Data Categories and Sharing Behavior

Contact Data (Name, Address, Telephone Number, E-mail, Mailing Lists)									
#	Question	20 - 25	26 - 30	31 - 35	36 - 40	40 - 45	46 - 50	51 - 55	Total
1	1+ times/week	8%	36%	31%	15%	7%	0%	3%	309
2	1+ times/month	7%	35%	35%	10%	13%	1%	0%	92
3	Rarely	7%	37%	40%	10%	0%	3%	3%	30
4	Don't know	0%	0%	0%	0%	0%	0%	0%	0
Non-health Data (Age, Sex, Weight, Height, etc.)									
#	Question	20 - 25	26 - 30	31 - 35	36 - 40	40 - 45	46 - 50	51 - 55	Total
1	1+ times/week	8%	35%	31%	14%	11%	0%	0%	108
2	1+ times/month	4%	36%	33%	16%	7%	3%	3%	76
3	Rarely	9%	36%	32%	13%	7%	0%	3%	247
4	Don't know	0%	0%	0%	0%	0%	0%	0%	0
Lifestyle (Interests, Hobbies, Taste, Passions)									
#	Question	20 - 25	26 - 30	31 - 35	36 - 40	40 - 45	46 - 50	51 - 55	Total
1	1+ times/week	7%	34%	33%	16%	7%	1%	2%	129
2	1+ times/month	11%	43%	24%	14%	6%	0%	2%	63
3	Rarely	7%	32%	37%	12%	9%	1%	2%	177
4	Don't know	10%	42%	26%	11%	8%	0%	3%	62
Opinions and Convictions (Religious Affiliation, Political Opinions, etc.)									
#	Question	20 - 25	26 - 30	31 - 35	36 - 40	40 - 45	46 - 50	51 - 55	Total
1	1+ times/week	9%	27%	36%	11%	14%	1%	1%	91
2	1+ times/month	11%	40%	26%	17%	3%	0%	3%	35
3	Rarely	7%	36%	33%	14%	6%	0%	2%	263
4	Don't know	10%	48%	21%	12%	7%	0%	2%	42

Web Data (Website Visits, Clicks, Posts, Likes, Comments, Cookies, etc.)									
#	Question	20 - 25	26 - 30	31 - 35	36 - 40	40 - 45	46 - 50	51 - 55	Total
1	1+ times/week	9%	37%	32%	13%	7%	0%	2%	294
2	1+ times/month	8%	31%	27%	22%	12%	0%	0%	49
3	Rarely	7%	38%	28%	13%	8%	2%	5%	61
4	Don't know	4%	30%	48%	4%	13%	0%	0%	23
Sensor Data (Smart Gadgets, Household Devices, etc.)									
#	Question	20 - 25	26 - 30	31 - 35	36 - 40	40 - 45	46 - 50	51 - 55	Total
1	1+ times/week	7%	37%	34%	14%	5%	1%	2%	135
2	1+ times/month	5%	37%	29%	17%	9%	0%	3%	76
3	Rarely	7%	35%	32%	14%	10%	1%	1%	167
4	Don't know	18%	33%	29%	9%	7%	0%	4%	45
Location Data (GPS Data, etc.)									
#	Question	20 - 25	26 - 30	31 - 35	36 - 40	40 - 45	46 - 50	51 - 55	Total
1	1+ times/week	8%	37%	33%	13%	7%	0%	2%	358
2	1+ times/month	10%	29%	29%	14%	19%	0%	0%	21
3	Rarely	4%	28%	26%	24%	9%	4%	4%	46
4	Don't know	0%	40%	60%	0%	0%	0%	0%	5

Appendix 3 – Segmentation of User Rights by Level of Importance

The summary table below concludes the respondent feedback on the level of importance of each user right, clustered by the scores and presented in a percentage column-wise distribution view.

Table 27: Segmentation of User Rights by Level of Importance

	Right to							
Score[a]	be informed	access data	data rectification	data erasure	restrict processing	data portability	object to data processing	object automated processing
0	4,0%	2,1%	0,9%	14,0%	6,3%	9,5%	8,8%	4,7%
1	0,2%	0,0%	6,3%	2,8%	15,6%	7,0%	0,0%	17,7%
2	37,0%	25,1%	5,6%	6,0%	10,5%	38,4%	6,5%	17,9%
3	58,8%	72,8%	87,2%	77,2%	67,7%	45,1%	84,7%	59,8%

[a]Score values read as follows: 0 = not important at all, 1= less important, 2= important, 3 = very important. Score value 1 is left out due to insignificance of available data. While this view allows a column-wise comparison, an absolute segmentation view, i.e., in proportion to the entire table sum is provided in appendix 3.

Appendix 4 – Detailed Information on GDPR Penalties from 2018 to 2022

Figure 31: Cumulative GDPR Penalties YoY Comparison from 2018 to 2022

The cumulative view of imposed fines presented in figure 30 shows the development of penalties over a time span of over 2.5 years, i.e., 28.05.2018 until 16.01.2022. In January 2022, a total of 993 unique fines were collected and analyzed for figure 31 and 32, amounting to 1.54 billion Euros. The cumulative view considers already effective and binding as well as issued penalties. The latter refers to investigations currently underway, which may change the actual and therefore final settlement amount. Further segmentation of fines is presented in Table 30 and 31 Fine Meta Data & Facts. At the time of the doctoral thesis, the fines presented are actual figures imposed by the local data protection authorities and may take effect in the event of an unsuccessful appeal by the concerned organizations.
The graph demonstrates that during this period, the fines grew in line with the exponential trendline, as indicated by the red line in the graph. The values highlighted by arrows show the cumulative penalty amount and the year-on-year growth at the turn of each year. The following table details the important fines of each year.

Table 28: Major GDPR Penalties from 2018 to 2022

Fine [in mil. Euro]	Year	Country	Organization	Summary
0.4	2018	Portugal	Centro Hospitalar Barreiro Montijo	Information security is not adequately protected by technical and organizational measures of the hospital (Monteiro, 2019)
50.0	2019	France	Google Inc.	A legal basis had not been established as consents had been given without any specifics or ambiguities
35.3	2020	Germany	H&M Hennes & Mauritz Online Shop A.B. & Co. KG	Private information about employees (incl. health condition) where stored and used by managers for the evaluation of employee performance, without employees knowledge
60.0	2021	France	Facebook Ireland Ltd.	Inadequate legal basis for data processing, as cookie management was not effective
150.0	2021	France	Google Ireland Ltd. and Google LLC	Fine is composed of multiple penalties due to inadequate legal basis for data processing, as cookie management was not effective on various websites operated by Google
225.0*	2021	Ireland	WhatsApp Ireland Ltd.	Fine is composed of multiple penalties for the violation of various GDPR articles, as information duties were not addressed sufficiently
746.0*	2021	Luxem-bourg	Amazon Europe Core S.à.r.l.	Lack of GDPR compliance with general data processing principles (Lintvedt, 2021, p.6)
8.0*	2022	Austria	REWE International AG	Lack of transparency in the scope of the usage of customer loyalty card information by the supermarket chain

*Ongoing investigation

Euro value of fines reflect the sum of all imposed GDPR related penalties since enforcement in May 2018 up to and incl. January 2022.

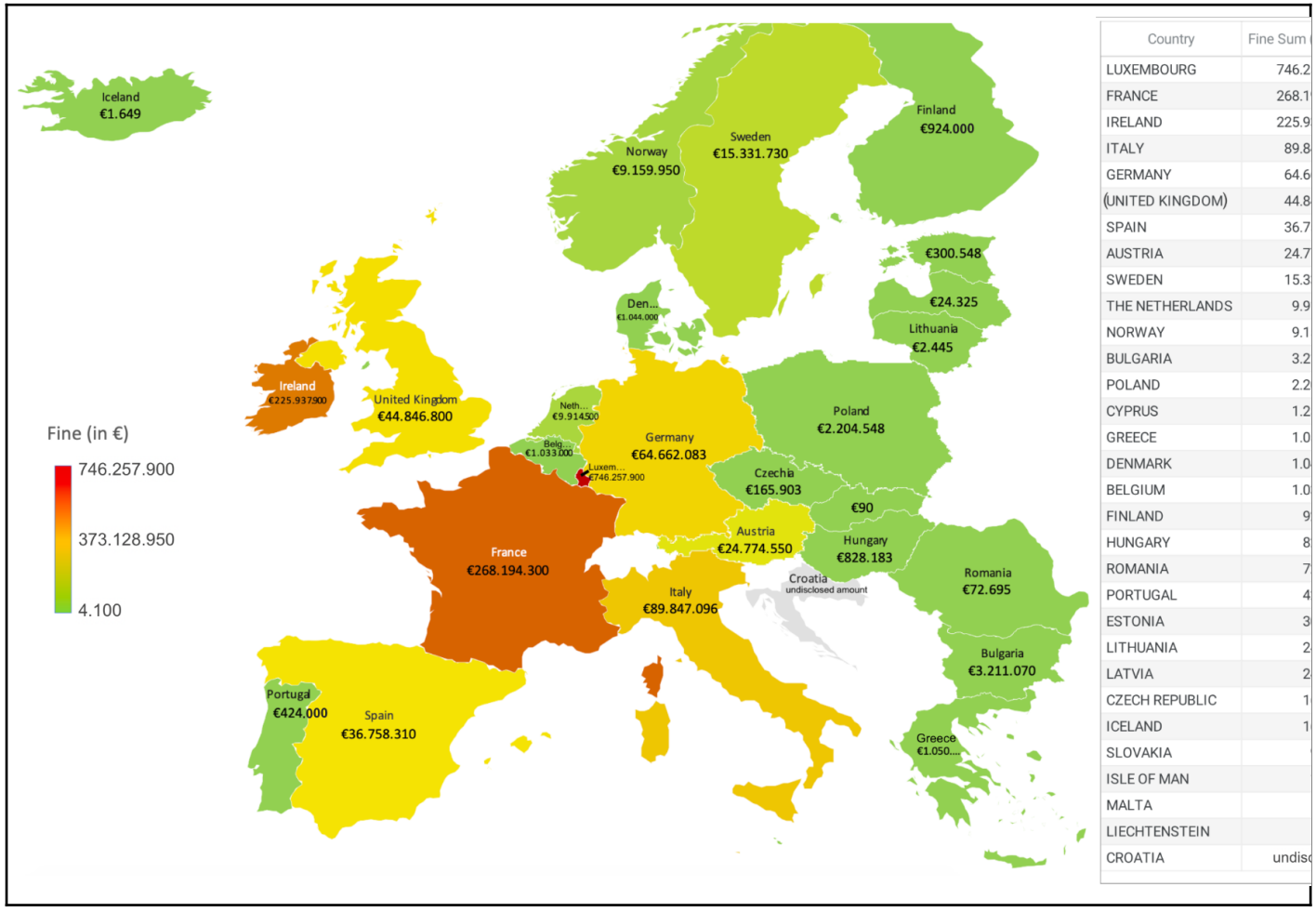

Figure 32: Map View of Cumulative GDPR Penalties 2018 - 2022 In the EU, incl. UK

Appendix 5 – Summary of Core Facts and Important Findings

Table 29: Summary Q&A for Research Undertaking

Question	Answer
What reduces complexity effectively?	1. Define purpose for data processing activities (i.e., use cases), 2. Understand the lifecycle (of personal data for each use case), 3. Minimize data (used in each use case), 4. Review processes (use cases), 5. Monitor personal data activities (use cases) and in all steps above ensure "baking in" end-to-end-lifecycle privacy design features and improving user awareness through effective UI/UX measures.
What are effective elements to achieve successful operationalization of the GDPR?	Privacy by design end-to-end-lifecycle proves to be an effective element. Based on the conceptual assessment, concrete measures are the use of just-in-time privacy notices, icons in smaller screens (e.g., smart watches), provisioning of hard copy of privacy modalities and QR codes. Create a trustworthy, fair, and transparent environment for processing data generated by or attributable to individuals and enforcing accountable handling of data by the data controller. UI/UX measures include the decrease of time-cost for reading privacy modalities, special attention on psychological measures and perceptions of users.
Conceptualization of a user-oriented online privacy control system possible and feasible (Y/N)? What are the success factors?	Yes, feasible. Psychological perspective may be the most significant as cultural and emotional values shape the perception of the level of control users can exercise on extraneous conditions and variables. Technological element provides concrete technical and organizational roadmap to operationalize legal requirements, which in turn facilitates the basis for meeting psychological requirements
What are the effects of a privacy control interface on organizational trustworthiness and control?	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 data type. Therefore, control over personal data via a privacy control system establishes and enhances organizational trustworthiness. In particular, control can be regarded as a foundation or an entry point for creating trustworthiness.
What leads to better control of personal information?	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 and length and interface design and navigation essentially influence the time cost.

Table 30: Research Meta Data & Facts

Meta Data	Figure	Specification
Total GDPR fines recorded and analyzed over a time span of four years:	4.095	fines (see Table 31 for details)
Total responses collected:	682	431, main survey 151, in preliminary study (user behavior reading privacy policy) 100 in preliminary study (democratizing your privacy)
Total unique data points collected and analyzed over a period of 3 years and 8 months:	75023	36.120 individual answers from main survey 151 in preliminary study (user behavior reading privacy policy) 1.500 in preliminary study (democratizing your privacy) 12.471 (fines*, 16.01.22) 3.612 (fines*, 05.08.21) 7.074 (fines*, 07.02.21) 6.238 (fines*, 09.12.20, incl. fines since 2018) 8.286 (fines*, reference database for quality assurance)
Total	76.698	Number of data points analyzed for the research

*Refers to the data points collected related to individual fines, i.e., each fine may consist of up to 10 data points.

Table 31: Fine Meta Data & Facts

Sector (Aggregated)	Fine Amount (Euro)
Media, Telecoms and Broadcasting	580.180.441
Industry and Commerce (Retail)	775.834.292
Transportation and Energy	53.335.369
Accommodation and Hospitality	21.461.207
Others	118.806.512
Total	1.549.617.821

Table 32: Survey Response Highlights

Insights of Survey Data	Figures
Device usership: most personal device	94% of all respondents own a personal smartphone
Age group distribution	Seven distinct age groups, the 26 - 30-year-olds account for 36% and the age group 31 - 35 make up 70%.
Most frequently shared personal data (self-reported by users)	Of all respondents' reports, the following data is shared: • 85% Location data (GPS data, etc.) • 80% Web data (website visits, clicks, posts, likes, comments, cookies, etc.)