

# The status-quo of companies' data privacy and security communication: An ethical evaluation and future paths

K. Valerie Carl <sup>1</sup>


**Abstract:** Advancing digital technologies and the omnipresent digitalization bear chances but also threats for companies and consumers. Especially data privacy and security risks remain one key concern of consumers. However, fulfilling legally binding requirements is not sufficient anymore for many consumers. Instead, consumers expect companies to behave ethically responsible and voluntarily assume more responsibilities in the digital context, particularly related to data privacy and security. Broader approaches, like the emerging concept of Corporate Digital Responsibility, make it possible to see responsibility with regard to data privacy and security in the broader context of a company's digital responsibilities and thus to develop a more holistic understanding. However, responsible behavior alone is not enough; rather an adequate communication is the evaluation basis of consumers. Accordingly, this work-in-progress evaluates current corporate communication regarding data privacy and security from an ethical view, thus illustrating best practices and paving future paths for corporate communication.

**Keywords:** data privacy, data security, company communication, best practices, communication guidelines, Corporate Digital Responsibility.

## 1 Introduction

The omnipresent digitalization and associated advanced digital technologies, products, and services transform private and professional lives. These advancements allow networks of devices to communicate via the Internet, exchange data, and to automate processes and tasks without human interferences. In this context, advancements in Artificial Intelligence (AI) and interconnectedness present an essential element of a plethora of products, services, and systems. Accordingly, a company's handling of the collected data is gaining in importance for, e.g., consumers and society; particularly since risks related to these activities are one of the key concerns of consumers [e.g., Ma86, MZH17]. Especially recently, and reinforced once again by the COVID-19 pandemic, consumers' awareness of data privacy and security has increased and, at the same time, so have their demands on companies to behave ethically and voluntarily exceed the minimum legally required responsibilities [IP18]. Nowadays, it is no longer sufficient for companies to comply with legal standards [Mi22]. Rather, the requirements for ethical behavior and corporate communication have increased to make ethical behavior visible. Hazards related to

---

<sup>1</sup> Goethe University Frankfurt/Main, Chair of Information Systems and Information Management, Theodor-W.-Adorno-Platz 4, D-60323 Frankfurt am Main, Germany, kcarl@wiwi.uni-frankfurt.de,   
<https://orcid.org/0000-0003-4655-1046>

unethical behavior result in economic, ethical, and legal issues for companies and consumers alike [Ba19]. Hence, data privacy and security activities of companies have the ability to positively or negatively influence a consumer's perception of a company, thus also technology adoption, with a lasting effect [Lu02]. Hence, it is of tremendous importance to direct companies' activities towards consumer requirements in this field. However, consumers are not aware of many activities. Rather they evaluate corporate communication and (mostly negative) incidents related to data privacy and security. Therefore, it is crucial for companies to align internal activities with their communication to exploit the full potential of additional efforts.

Still, firms struggle to keep up with the requirements for more ethical communication and behavior due to the lack of guidelines and best practices. Yet, standards guide socially responsible behavior (i.e., Corporate Social Responsibility (CSR)), however, with regard to data privacy and security, without concrete guidance for companies and current standards lack an adequate emphasis on this distinct topic [CZH22]. Nevertheless, there is a vast amount of research addressing data privacy and security in general [e.g., BC11, HH18] and its effect on technology adoption [e.g., Lu02]. Still, research lacks the link to an ethical evaluation of corporate activities and their communication in the digital era. One evolving concept aiming at the support of ethical digital behavior of companies is the concept of Corporate Digital Responsibility (CDR). This concept allows for a broader perspective on responsibilities related to (digital) corporate activities (e.g., data privacy and security activities). CDR and CSR both sum up to the broader concept of Corporate Responsibilities and address different aspects of a broader responsibility understanding. CSR targets social and economic impacts of corporate activities [MR02], whereas CDR puts digital responsibilities in the focus. Digital responsibilities relate to the exploitation of opportunities and the handling of potential negative outcomes of digitalization [Lob21, Mi21]. The concept of CDR subsumes yet rather isolated aspects of digital responsibilities in the bigger picture to ensure a more holistic understanding of corporate responsibilities in the digital era, aiming at enhanced consumer trust in corporate activities. Thus, the concept provides a framework not only for ethically responsible corporate activities but also for making them visible to consumers through appropriate corporate communication. In this way, communication regarding data privacy and security activities can benefit from putting associated responsibilities into the larger context to support consistent communication and enhanced consumer trust.

Nevertheless, CDR and its practical implementation are still in its infancy [Lob21] although consumers already expect ethically responsible behavior from firms. By now, we can observe an increasing discourse in research [e.g., Lob21], practice [e.g., He21], and from regulatory entities [e.g., Th17] related to the concept of CDR. However, the focus lies currently on developing a common understanding of CDR and its scope [e.g., He21, Lob21, Mi21]. Yet, concrete guidance for ethically responsible company communication, especially directed at data privacy and security activities, lacks. Therefore, primarily small and medium sized enterprises (SME) struggle when fostering a more ethical communication due to missing guidelines and best practices. Hence, it is of tremendous importance to provide further guidance especially for SME. In general, individual

consulting by consulting firms is not feasible for ethical communication in most SME unlike for larger companies. Thus, this study aims to close this gap and provides guidance on the ethically responsible communication related to data privacy and security by pointing out possible best practices and positive examples.

To achieve this goal, this study evaluates companies' data privacy and security communication to propose some best practices and to indicate future paths for a more ethical communication. Section two introduces data privacy and security responsibilities. Subsequently, the next sections present the study design and the results of the study, before drawing a conclusion and presenting an outlook and this study's implications. To derive best practices and therefore guidance on an ethical communication, the focus on business-to-consumer (B2C) companies compared to business-to-business (B2B) companies is necessary. B2C and B2B companies differ in terms of their stakeholders' demands regarding behavior and corporate communication, which makes them harder to compare. Accordingly, this study initially focuses on B2C companies for the development of best practices. B2C companies face communication needs of a variety of stakeholders (e.g., employees, consumers, society). Since consumers are increasingly sensitive to ethical behavior or the lack thereof, we selected consumers as the addressees of corporate communication. Hence, this study is concerned with B2C companies and specifically with their communication directed at consumers.

## **2 Data Privacy and Security Responsibilities**

In general, data privacy addresses consumers' control over data usage, including but not limited to storing, processing, and forwarding of consumer data. By contrast, data security describes the protection of consumer data against (virtual) attacks and other threats [BC11]. Hence, in the digital economy, the monetization of consumer data, data use, possible control over it, and information security are in the focus of consumer concerns [e.g., BC11, We67]. Regulations define the minimum requirements for data privacy and security activities in many countries (e.g., for companies to which the GDPR applies). Compliance with these regulations does not stand out positively whereas non-compliance can have severe financial and legal consequences [e.g., GS09]. Against this background, companies have to exceed legal regulations to positively influence a consumer's perception of a company [Ha07]. Voluntarily assuming additional responsibility in the digital context, especially with regard to data privacy and security, is becoming increasingly important for companies and, above all, making this behavior visible to consumers – usually by communicating such activities. The topic of data privacy and security is multifaceted and does not occur isolated from further responsibilities in the digital era. Accordingly, a concept such as CDR can help to put these responsibilities into context and thus track consistent communication regarding digital responsibilities. This also favors the communication of data privacy and security related activities and creates a certain credibility and consumers' trust. Within the context of CDR, ethically responsible behavior and communication related to data privacy and security forms one dimension of

the concept [e.g., Th17, Mi21] and comprises various fields of action. Several different classification approaches developed in parallel. In order to keep the complexity bearable for practitioners, this study employs a classification based on the four privacy areas according to Smith et al. [SMB96] and current legislation (e.g., GDPR, OECD guidelines [Oe13]). Table 1 summarizes the data privacy and security fields of action according to the concept of CDR.

<b>Fields of action</b>	<b>Description</b>	<b>Related work</b>
<i>Data privacy and security fields of action</i>		
Openness	Openness describes the degree to which companies are open with consumers, especially with regard to data processing practices.	GCC15, THS08
Data collection	Data collection covers limited data collection and the clear purpose of data collection.	GCC15, THS08
Data processing	Data processing comprises restricted data use as well as secure storage and processing of data.	BC11, GCC15
Data management	Data management refers to data quality of user data (e.g., accurate, up-to-date) and consumers' access and correction opportunities.	SK08, SMB96
<i>Further data privacy and security related fields of action within the concept of CDR</i>		
Transparency on internal governances	Transparency on internal data privacy and security governances describes the disclosure of internal practices to consumers.	ABK17, MW10
Transparent communication on internal practices	A transparent communication on data privacy and security addresses additional information on data transmission practices and a transparent and easy to understand data protection declaration.	BC11, GS09
Access without data input	Access without data input describes consumers' ability to access products and services (e.g., advisory services) without entering personal data.	BC11, SK08

Tab. 1: Data privacy and security fields of action within the concept of CDR

### 3 Study Design and Sample

To derive best practices on ethically responsible data privacy and security communication we rely on qualitative text analysis. Therefore, we quota sampled on companies operating in Germany from different industries and with varying digital products and services. The sample is limited to companies operating in Germany due to the already high legal and regulatory requirements for corporate communication on data privacy and security and the increased awareness of consumers. With the inclusion of varying products and industries, this study aims at creating a cross-industry understanding of ethically responsible

corporate communication in this field. To derive best practices and therefore guidance, we rely on the communication of large companies as they usually have a larger budget available for possible activities and their communication. Besides, larger companies primarily participate in initiatives for more ethical behavior. When looking at industry initiatives (e.g., the Bundesverband Digitale Wirtschaft e.V.) as well as governmental initiatives (e.g., the CDR Initiative of the German Federal Ministry for the Environment, Nature Conservation, Nuclear Safety, and Consumer Protection), it is mainly larger companies that participate to set new industry standards. Hence, we included companies with such a visible CDR commitment primarily in the sample, as their motivation is the setting of best practices. Accordingly, they can mostly be used for such, especially at such an early stage of CDR implementation in practice. Hence, we selected a sample of 26 companies (see Table 2) based on the targeted criteria. We crawled potentially relevant corporate communication from the website and qualitatively analyzed them. The documents range from legal documents (e.g., data protection declarations) to voluntary communication of corporate responsibility. Only publicly available documents were included in the sample<sup>2</sup>, as only these are accessible to consumers. Therefore, this study excludes company internal documents not available for people outside the company. We collected the data in fall 2021 to draw a recent picture of corporate communication on data privacy and security.

<b>Industry<sup>3</sup></b>	<b>Company</b>
Automotive	BMW Group, Continental AG, Mercedes-Benz Group, Volkswagen AG
Banking and financial services	HSBC Trinkaus & Burkhardt AG, ING Bank N. V., SCHUFA Holding AG
Computer hardware & software	IBM Corporation, Microsoft Corporation
Cosmetics & pharmacy	L'Oréal Groupe, Merck KGaA
Electrical appliances	Miele & Cie. KG, Philips GmbH Market DACH, Robert Bosch GmbH, Siemens AG, Sony Group, Vorwerk SE & Co. KG
Insurance	BARMER, Zurich Insurance Group Ltd
Retail and consumer services	Otto Group, Rewe Group, Zalando SE
Telecommunication	Deutsche Telekom AG, Telefónica S.A., Vodafone Group Plc
Utilities	EWE AG

Tab. 2: Companies in the study sample

We used MAXQDA for the qualitative analysis of corporate communication. No traditional coding scheme matches the topic under investigation. Hence, we developed a coding scheme according to established guidelines for thematic qualitative text analysis [Ku14, pp. 69ff.] and accordingly developed our codebook during the coding process.

<sup>2</sup> The study analyzed 766 documents in total, thus in average 29 documents per company.

<sup>3</sup> Assignment based on industry affiliation usually known to the consumer.

Three independent researchers performed the coding in parallel to discuss and contrast coding results. This ensures an adequate quality of results [VBS16]. The team reviewed conflicts in coding and solved them in mutual agreement, thus systematically developing and adapting the codebook. An external coder with prior coding experience assessed the coding results to ensure semantic quality and agreed with the assignments.

## 4 Results

Our findings indicate that most information on data privacy and security related activities is of a legal nature and less about the company assuming additional responsibility towards the consumer. However, for example in the EU, the websites under consideration are also required to publish (legal) privacy statements. Nevertheless, in the course of assuming additional responsibility on a voluntary basis, companies can provide additional documents and website content that exceeds these legal requirements. Addressing these additional responsibilities, this work-in-progress takes a closer look at possible best practices for data privacy and security related corporate communication under the concept of CDR. The aim of the study is to identify some examples of additionally assumed responsibility per data privacy and security field of action and thus to provide guidance for researchers and practitioners alike on responsible corporate communication. However, this study does not intend to provide an all-encompassing catalogue of possible best practices or to provide a comparison between the investigated companies. Accordingly, the frequency of the companies cited should not be used to evaluate a company's corporate communication. Rather, each field of action comprises various possible corporate communication examples that represent best practices. In the following, exemplary activities in corporate communication are illustrated for the various fields of action and best practices are discussed. Communication best practices should also serve as guidelines for ethical behavior, ensuring that communication and internal behavior are aligned.

The field of action related to openness describes responsible acting of companies by disclosing their data processing practices openly in the course of additional information [e.g., GCC15, THS08]. For instance, companies can provide additional website content addressing further, more comprehensible openness about data protection practices also disclosing precisely what the data is used for: *“For example, insights from the data will enable Zurich to provide innovative services that help to prevent incidents, expanding the traditional protection offered by insurance. These include smart services for home protection, and to improve health and well-being, as well as travel that keeps customers out of harm's way.”* [Zu21]. In a similar vein, companies can aggregate the main purposes for which consumer data is used, thus demonstrating greater openness to consumers: *“Key uses of customer data are outlined below. [...]”* [Vod21]. Such openness supports companies' responsible communication towards consumers about their data processing practices and thus informed consumer decision making.

Data collection concerns limited or restricted data collection on the one hand and the clear

purpose of data collection on the other hand [e.g., GCC15, THS08]. For example, companies can address this additionally assumed responsibility by providing additional website content explaining limited data collection practices: “[W]e gather only the data that is absolutely essential, [...] as well as ensuring transparency vis-à-vis the customer.” [De21]. Besides, companies can explain and communicate their default settings of products and services regarding (limited) data collection: “[A]ppiances are shipped out with default settings that ensure the highest degree of data minimisation. Any communication or data transfer that goes beyond this must be explicitly activated by the customer.” [Mie21]. Especially the application of more advanced systems, like AI-based systems, deepen the necessity of taking responsibility with regard to data collection. For instance, companies should therefore address these consumer concerns, disclosing their internal obligation for limited and purposeful data collection: “The aggregation and use of customer data – especially in AI systems – shall always be clear and serve a useful purpose towards our customers.” [De21]. Corporate communication geared to these demands are evidence of more ethical corporate behavior.

Data processing practices address manifold facets of responsible behavior including handling of secondary usage, transfer of data to third parties, or secure processing and storage of data, therefore presenting another important field of action [e.g., BC11, GCC15]. Thus, companies can assume additional responsibilities in manifold ways, e.g., offering information on data processing to third parties as additional website content: “Further, any third party with whom Zurich does share personal data is bound by an enforceable contract, which sets out how that personal data can be used.” [Zu21, see also Ph21]. Besides, additional information and even possible ways of contacting regarding secure storage and processing of data is another path to assume more responsibility regarding data processing: “But we are extremely conscious of our responsibilities to all our stakeholders and work diligently to secure business assets and information, especially data protected under the law and sensitive information under antitrust law. [...] We always comply with the processes on data and information security. We expect you to ask for advice with the Privacy & Technology Law team (it-law-intern@zalando.de) whenever you are in doubt.” [Za21, see also Ph21]. Another approach is to inform in detail about data processing and securing mechanisms like the privacy by design process applied internally to product and service development [Te21]. Besides, companies can provide additional information on certifications or passed security tests: “In this context, we at Vorwerk are proud to be the winners of independent tests on data security. For example, most recently in January 2019, the Kobold VR300 Vacuum Robot won the security check undertaken by the independent IT security institute AV-TEST.1.” [Vor21, see also Ot21]. Hence, due to the many different aspects of responsible data processing, there are also many different approaches for companies to communicate ethical behavior.

Another field of action, precisely data management, covers data quality as well as consumers’ access to their stored data [e.g., SK08, SMB96]. Therefore, companies acting ethically responsible can pursue and communicate to consumers that they “[m]anage data carefully” including to “[m]aintain data quality, delete unnecessary or outdated data and do not take unnecessary copies.” [Vod21, see also Hs21, In21, Sc21]. Besides, companies

should facilitate and communicate consumers' access and deletion rights to their data stored: “[We d]esign products to allow individuals to exercise their right to access, request deletion and portability.” [Vod21]. This approach also includes to “[e]mpower our customers through simple and secure tools so that they can control the use of their personal data.” [Te21, see also In21, Ph21, Ro21], therefore respecting individual rights related to stored data.

Besides, companies can voluntarily provide transparency regarding internal governances affecting data privacy and security activities [e.g., ABK17, MW10]. For instance, companies can disclose internal governances directly addressing their data privacy and security related activities, e.g., “[we] have created, among other things, a uniform international framework for this in the shape of our Binding Corporate Rules Privacy. These define the purposes for which personal data may be collected, stored and processed. We endeavor to clarify any unresolved questions or issues without delay. We set ourselves principles early on for new business models, which make it clear to our customers, employees and business partners how we deal with these models and leave them in no doubt that we assume responsibility.” [De21] or disclosing additional information on their risk management principles related to data privacy and security: “The Zurich Risk Policy, applied across the Group, lays down the Group’s risk management principles. There is a dedicated section on Information Security supported by detailed policy manuals, guidelines and standards including those for data handling and classification of assets and information.” [Zu21, see also Ph21] accompanied by associated training material [Ew21, Sc21, Si21, Vor21]. Besides, companies also establish own codes of ethics to ensure ethical behavior in general [Ba21, Lor21, MK21, Re21, Ro21, Si21, Za21], specific AI guidelines for ethical AI deployment and usage [Bm21, Co21, De21, Ib21, Mic21, Re21, Ro21, So21], or CDR guidelines [Sc21]. Internal governances also include the disclosure of specific boards [MK21] or committees [Ph21] established to foster additional data privacy and security activities: “We particularly focus on maintaining information security and defending against cyber attacks. The Group Information Security Steering Committee (GISSC) [...] has overarching responsibility.” [Vol21]. By disclosing such internal governances, practices, and initiatives, companies can prove ethically responsible behavior and transparently communicate it to consumers.

Earlier research has already addressed the need for more understandable privacy statements for a considerable time [e.g., BC11, GS09]. Nevertheless, there has not been that much progress yet in this field and many companies leave it primarily to the publication of the legally binding privacy policies. This is reflected above all in relatively long privacy statements, which are also worded in a rather complicated manner and thus do not allow consumers to easily understand the data distribution, collection, and management practices. However, some companies already make some effort to provide easier to understand additional documents. For example, companies can provide a “one-pager”: *an easy-to-read, brief overview of the main data processing activities*” [De21, see also MB21]. Such a one-pager facilitates consumers' access to relevant data privacy and security activities of a company and thus provides a reasonable approach to additional assumption of responsibility in the digital context. In addition, there are discussions in



public about using data protection icons to ensure easier access to data protection declarations. Yet, such an approach could not be observed in the sample studied.

Another field of action concerns access to digital services or products without data input [e.g., BC11, SK08]. Companies can offer access to several digital products and services without requiring the disclosure of personal data. This additional responsibility is applicable to a wide range of services and products and also includes, e.g., the topping up of credit without disclosing personal data: *“Provides a dummy ten-digit number to ensure the privacy of customers when they recharge at retail outlets, avoiding the need for them to have to reveal their mobile number to an unknown retailer.”* [Vod21]. Activities and corporate communication related to this field of action can reduce consumers’ privacy concerns, as disclosure of personal data is not forced.

## 5 Conclusion and Outlook

As results illustrate, we can already find a vast set of best practices regarding data privacy and security corporate communication. Therefore, it is of tremendous importance for companies of all sizes and industries to engage in the assumption of additional digital responsibilities and to address this topic in the future. This work-in-progress can serve as a first starting point for future paths and inspiration for ethically responsible corporate communication related to data privacy and security. Best practices could be identified in various data privacy and security fields of action that can guide future paths of corporate communication. By providing an ethical evaluation of the status-quo of corporate communication related to data privacy and security, this study benefits researchers and practitioners alike. Theoretically, this work in progress supports the understanding of ethically responsible corporate communication on data privacy and security. Besides, this study emphasizes the comprehensive scope of data privacy and security related activities when viewed in the larger context of concepts such as CDR. Practically, this study serves as a starting point for various companies with a B2C focus for a more ethically responsible corporate communication and therefore future paths for implementing additional activities or communicating already performed endeavors. However, ethically responsible communication does not always mean ethical behavior. While corporate communication can be ethically responsible, a company's behavior can still be unethical. Besides, companies (often) focus more on their own needs than on the ethically responsible treatment of consumer interests. Accordingly, this work aims to promote not only ethically responsible communication but also appropriate behavior and to reinforce the importance of it.

Despite best efforts, this study is not without limitations. The sample is limited to companies operating in Germany, especially B2C companies, and their communication addressing consumer concerns. Hence, future research should add to the derived best practices and future paths for data privacy and security communication by including companies from different countries. Besides, B2B companies and other stakeholders of

companies (e.g., employees) should complement a broader understanding of best practices in corporate communication. Nevertheless, this study can provide a first starting point for theory and practice for a more ethically responsible data privacy and security behavior and its communication, thus providing first guidance on the this topic.

## Acknowledgement

The Hessian State Chancellery – Hessian Minister of Digital Strategy and Development supported this work under the promotional reference 6/493/71574093 (CDR-CAT).

## Bibliography

- [ABK17] Anderson, C.; Baskerville, R. L.; Kaul, M.: Information Security Control Theory: Achieving a Sustainable Reconciliation Between Sharing and Protecting the Privacy of Information. *Journal of Management Information Systems* 34/4, pp. 1082-1112, 2017.
- [Ba19] Baumann, A.; Haupt, J.; Gebert, F.; Lessmann, S.: The Price of Privacy: An Evaluation of the Economic Value of Collecting Clickstream Data. *Business & Information Systems Engineering* 61/4, pp. 413-431, 2019.
- [Ba21] BARMER, <https://www.barmer.de/en>, accessed: 29/10/2021.
- [BC11] Bélanger, F.; Crossler, R. E.: Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly* 35/4, pp. 1017-1041, 2011.
- [Bm21] BMW Group, <https://www.bmwgroup.com/en.html>, accessed: 29/10/2021.
- [Co21] Continental AG, <https://www.continental.com/en/>, accessed: 29/10/2021.
- [CZH22] Carl, K. V.; Zilcher, T. M. C.; Hinz, O.: Corporate Digital Responsibility and the Current Corporate Social Responsibility Standard: An Analysis of Applicability. In: *Proceedings of the Open Identity Summit 2022 (OID2022)*, 2022.
- [De21] Deutsche Telekom AG, <https://www.telekom.com/en>, accessed: 29/10/2021.
- [Ew21] EWE AG, <https://www.ewe.com/>, accessed: 29/10/2021.
- [GCC15] Greenaway, K. E.; Chan, Y. E.; Crossler, R. E.: Company Information Privacy Orientation: A Conceptual Framework. *Information Systems Journal* 25/6, pp. 579-606, 2015.
- [GS09] Goel, S.; Shawky, H. A.: Estimating the Market Impact of Security Breach Announcements on Firm Values. *Information & Management* 46/7, pp. 404-410, 2009.
- [Ha07] Hann, I.-H.; Hui, K.-L.; Lee, S.-Y. T.; Png, I. P. L.: Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach. *Journal of Management Information Systems* 24/2, pp. 13-42, 2007.
- [He21] Herden, C.; Alliu, E.; Cakici, A.; Cormier, T.; Deguelle, C.; Gambhir, S.; Griffiths, C.; Gupta, S.; et al.: “Corporate Digital Responsibility”: New Corporate Responsibilities in

- the Digital Age. Sustainability Management Forum 29, pp. 13-29, 2021.
- [HH18] Heimbach, I.; Hinz, O.: The Impact of Sharing Mechanism Design on Content Sharing in Online Social Networks. *Information Systems Research* 29/3, pp. 592-611, 2018.
- [Hs21] HSBC Trinkaus & Burkhardt AG, <https://www.about.hsbc.de/>, accessed: 29/10/2021.
- [Ib21] IBM Corporation, <https://www.ibm.com/us-en?lnk=fcc>, accessed: 29/10/2021.
- [In21] ING Bank N. V., <https://www.ing.com/Home.htm>, accessed: 29/10/2021.
- [IP18] Intezari, A.; Pauleen, D. J.: Conceptualizing Wise Management Decision-Making: A Grounded Theory Approach: Conceptualizing Wise Management Decision-Making. *Decision Sciences* 49/2, pp. 335-400, 2018.
- [Ku14] Kuckartz, U.: *Qualitative Text Analysis: A Guide to Methods, Practice & Using Software*. Sage Publications, London & Thousand Oaks, 2014.
- [Lob21] Lobschat, L.; Mueller, B.; Eggers, F.; Brandimarte, L.; Diefenbach, S.; Kroschke, M.; Wirtz, J.: Corporate Digital Responsibility. *Journal of Business Research* 122, pp. 875-888, 2021.
- [Lor21] L'Oréal Groupe, <https://www.loreal.com/en/>, accessed: 29/10/2021.
- [Lu02] Luo, X.: Trust Production and Privacy Concerns on the Internet: A Framework Based on Relationship Marketing and Social Exchange Theory. *Industrial Marketing Management* 31/2, pp. 111-118, 2002.
- [Ma86] Mason, R. O.: Four Ethical Issues of the Information Age. *MIS Quarterly* 10/1, pp. 5-12, 1986.
- [MB21] Mercedes-Benz Group, <https://group.mercedes-benz.com/en/>, accessed: 29/10/2021.
- [Mic21] Microsoft Corporation, <https://www.microsoft.com/en-us/>, accessed: 29/10/2021.
- [Mie21] Miele & Cie. KG, <https://www.miele.com/en/com/index.htm>, accessed: 29/10/2021.
- [Mi21] Mihale-Wilson, A. C.; Zibuschka, J.; Carl, K. V.; Hinz, O.: Corporate Digital Responsibility – Extended Conceptualization and a Guide to Implementation. In: *Proceedings of the European Conference on Information Systems (ECIS) 2021*, 2021.
- [Mi22] Mihale-Wilson, A. C.; Hinz, O.; van der Aalst, W.; Weinhardt, C.: Corporate Digital Responsibility: Relevance and Opportunities for Business and Information Systems Engineering. *Business & Information Systems Engineering* 64/2, pp. 127-132, 2022.
- [MK21] Merck KGaA, <https://www.merckgroup.com/en>, accessed: 29/10/2021.
- [MR02] Maignan, I.; Ralston, D. A.: Corporate Social Responsibility in Europe and the U.S.: Insights from Businesses' Self-Presentations. *Journal of International Business Studies* 33/3, pp. 497-514, 2002.
- [MW10] Mingers, J.; Walsham, G.: Toward Ethical Information Systems: The Contribution of Discourse Ethics. *MIS Quarterly* 34/4, pp. 833-854, 2010.
- [MZH17] Mihale-Wilson, A. C.; Zibuschka, J.; Hinz, O.: About User Preferences and Willingness to Pay for a Secure and Privacy Protective Ubiquitous Personal Assistant. In: *Proceedings of the European Conference on Information Systems (ECIS) 2017*,

pp. 32-47, 2017.

- [Oe13] OECD, [http://www.oecd.org/sti/ieconomy/oecd\\_privacy\\_framework.pdf](http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf), accessed: 09/07/2019.
- [Ot21] Otto Group, <https://www.ottogroup.com/en/>, accessed: 29/10/2021.
- [Ph21] Philips GmbH Market DACH, <https://www.philips.com/global>, accessed: 29/10/2021.
- [Re21] Rewe Group, <https://www.rewe-group.com/en/>, accessed: 29/10/2021.
- [Ro21] Robert Bosch GmbH, <https://www.bosch.com/>, accessed: 29/10/2021.
- [Sc21] SCHUFA Holding AG, <https://www.schufa.de/schufa-en/>, accessed: 29/10/2021.
- [Si21] Siemens AG, <https://www.siemens.com/global/en.html>, accessed: 29/10/2021.
- [SK08] Son, J.-Y.; Kim, S. S.: Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model. *MIS Quarterly* 32/3, pp. 503-529, 2008.
- [SMB96] Smith, H. J.; Milberg, S. J.; Burke, S. J.: Information Privacy: Measuring Individuals' Concerns About Organizational Practices. *MIS Quarterly* 20/2, pp. 167-196, 1996.
- [So21] Sony Group, <https://www.sony.com/en/>, accessed: 29/10/2021.
- [Te21] Telefónica S.A., <https://www.telefonica.com/en/>, accessed: 29/10/2021.
- [Th17] Thorun, C.; Vetter, M.; Reisch, L.; Zimmer, A. K., [https://www.bmjv.de/G20/DE/ConsumerSummit/\\_documents/Downloads/Studie.pdf?\\_blob=publicationFile&v=1](https://www.bmjv.de/G20/DE/ConsumerSummit/_documents/Downloads/Studie.pdf?_blob=publicationFile&v=1), accessed: 09/07/2019.
- [THS08] Tang, Z.; Hu, Y.; Smith, M. D.: Gaining Trust Through Online Privacy Protection: Self-Regulation, Mandatory Standards, or Caveat Emptor. *Journal of Management Information Systems* 24/4, pp. 153-173, 2008.
- [VBS16] Venkatesh, V.; Brown, S.; Sullivan, Y.: Guidelines for Conducting Mixed-methods Research: An Extension and Illustration. *Journal of the Association for Information Systems* 17/7, pp. 435-494, 2016.
- [Vod21] Vodafone Group Plc, <https://www.vodafone.com/>, accessed: 29/10/2021.
- [Vol21] Volkswagen AG, <https://www.volkswagenag.com/en.html>, accessed: 29/10/2021.
- [Vor21] Vorwerk SE & Co. KG, <https://www.vorwerk-group.com/en/home>, accessed: 29/10/2021.
- [We67] Westin, A. F.: *Privacy and Freedom*. 1st. ed. Athenum, New York, 1967.
- [Za21] Zalando SE, <https://corporate.zalando.com/en>, accessed: 29/10/2021.
- [Zu21] Zurich Insurance Group Ltd, <https://www.zurich.com/en>, accessed: 29/10/2021.