Friesenecker, Matthias; Gotsch, Mauro Luis; Schögel, Marcus

Article

Knowing is Half the Battle - The Influence of Marketers' Privacy Literacy on SMEs' Privacy Orientation

Marketing Review St.Gallen

Provided in Cooperation with:
Universität St. Gallen, Institut für Marketing und Customer Insight

Suggested Citation: Friesenecker, Matthias; Gotsch, Mauro Luis; Schögel, Marcus (2022) : Knowing is Half the Battle - The Influence of Marketers' Privacy Literacy on SMEs' Privacy Orientation, Marketing Review St.Gallen, ISSN 1865-7516, Thexis Verlag, St.Gallen, Vol. 39, Iss. 2, pp. 36-43

This Version is available at:
https://hdl.handle.net/10419/276181

Marketingzeitschrift für Theorie & Praxis 2/2022

Marketing Review St. Gallen

Privacy as Strategy?

Schwerpunkt

Spektrum

Universität St.Gallen

Knowing is Half the Battle

The Influence of Marketers' Privacy Literacy on SMEs' Privacy Orientation

Marketers are in a unique position to improve customers' data privacy but often lack the necessary know-how. Hence, this study examines the link between marketers' privacy literacy and their firms' privacy orientation.

Matthias Friesenecker, B.A., Mauro Luis Gotsch, M.A., Prof. Dr. Marcus Schögel

While large enterprises like Google, Amazon, Facebook, Apple or Microsoft are under intense scrutiny regarding their data privacy practices (see, e.g., Stuart, 2021), comparatively little attention has been paid to the privacy practices of small and medium-sized enterprises (SMEs). Naturally, SMEs generally collect and utilize fewer customer data and have access to less advanced analytical capabilities (Bianchini & Michalkova, 2019). As a result, research regarding SME privacy practices and IT security has so far been "largely neglected" (Heidt et al., 2019, p. 1286). As SMEs' capabilities and access to data processing tools (e.g., AI-aided customer relationship management software) are expected to increase (Bianchini & Michalkova, 2019; Coleman et al., 2016; Sen et al., 2016), this knowledge gap could become a risk factor. In light of far-reaching privacy regulations such as the General Data Protection Regulation of the EU (GDPR) and the "exceptional vulnerability" of SMEs to cyberattacks (Van Haastrecht et al., 2021, p. 1), more research to understand and improve SMEs' privacy orientation is needed. Since SMEs tend to be more "resource constrained" (Hernández-Linares et al., 2021, p. 179), potential solutions should build upon already existing capabilities or functions.

Past research has showcased a variety of approaches to improve a firm's privacy orientation, and marketing as a function "is often specifically named as being the central node of the modern privacy debate" (Gotsch & Schögel, 2021, p. 24). In SMEs, marketing capabilities are both used to "attain superior business results" (Lekmat et al., 2018, p. 213) and are often concentrated in the hands of a few natural persons (Camra-Fierro et al., 2012). This means that the control of data-collecting touchpoints like websites is often directly shaped by a single person or a small team. SME marketers are therefore in a unique position to both specify their firm's informational needs so as to reduce surplus data collection (Zuboff, 2019) and to ensure the customers' desired data privacy throughout their journey. Yet, to utilize this potential it is likely that SME marketers need a basic level of privacy literacy (Baruh et al., 2017). Hence, this study aims to answer the following question:

RQ: *Does the privacy literacy of marketers working in a business-to-consumer SME influence the privacy orientation of their firm's website and the overall privacy policy?*

A quantitative approach following a three-step procedure was chosen to provide first insights into the link between the privacy literacy of marketers and the privacy orientation of the SMEs they are working for. In a first step, the privacy literacy of SME employees with influence on their firm›s touchpoints was recorded using a structured online questionnaire. In a second step, the corresponding privacy statements and websites were analysed. This was done on the basis of the legal minimum requirements defined by the GDPR and recorded by means of a structured evaluation form. Finally, the link between privacy literacy and data protection orientation of the website was tested using a multiple regression approach and an analysis of variance (ANOVA).

Theoretical Basis

Nissenbaum (2009, p. 4) defines informational privacy as a "claim to appropriate flows of personal information" within the "distinctive social context" of a customer–firm interaction. Hence, for an SME's privacy policy to be "privacy-oriented", it should allow the customer to easily view and adjust the level of how much they can be "sensed" by said SME through the data shared with them (Belanger et al., 2002, p. 245; Parker, 1974, p. 273; Petronio, 2010, p. 179).

While most modern data privacy laws set a baseline of protection which should be upheld by any entity collecting data ("privacy by design", GDPR, Art. 25), the sharing of personal data is still largely treated as a matter of personal responsibility. Yet, consent-driven privacy self-management faces the "inherent limitation" (Barocas & Nissenbaum, 2014, p. 31; Solove, 2013, 2021) of most customers being unable to overcome the "rational, irrational and structural" factors influencing their decision-making process (Gotsch & Schögel, 2021, p. 4). As a result, customers' expressed privacy concerns often do not match their level of disclosed personal data across various platforms (Acquisti, 2004; Norberg & Horne, 2007).

This limitation can be partially addressed by increasing the privacy literacy of all the parties involved. Trepte et al. (2015, p. 339) elaborate on this notion and state that privacy literacy is a combination of factual or declarative («knowing that») and procedural («knowing how») knowledge regarding the protection of one's data privacy.

Matthias Friesenecker, B.A.
MindShare AG,
Zürich, Switzerland
matthias.friesenecker@gmail.com

Mauro Luis Gotsch, M.A.
Institute for Marketing and Customer Insight, University of St. Gallen, Switzerland
mauro.gotsch@unisg.ch

Prof. Dr. Marcus Schögel
Institute for Marketing and Customer Insight, University of St. Gallen, Switzerland
marcus.schoegel@unisg.ch

Generally, increasing privacy literacy within a firm's human resource pool has been recommended by several studies as a means to achieve a higher privacy orientation (Amiri et al., 2018; Bulgurcu et al., 2017; Gotsch & Schögel, 2021; Kokolakis, 2017; Schögel, 2016; Solove, 2013; Taneja et al., 2014). However, the link between marketers' privacy literacy and touchpoint privacy orientation has not been established so far. This study aims to test the feasibility of this recommendation within the SME context where such a connection is more direct than in a large firm. Hence, we hypothesize:

H1: *The presence of SME marketers with high privacy literacy will increase the privacy orientation of the touchpoints under their influence.*

Since the decision to collect personal data from customers is expected to follow a rational weighing of customer risks and benefits, it is assumed that marketers perform a privacy calculus similar to that of their customers (Dinev & Hart, 2006; Zhu et al., 2017). To properly assess both the benefits and risks of their customers' disclosure of data, marketers need a certain level of privacy literacy (Trepte et al., 2015).

H2a: *SME marketers' privacy literacy positively affects the perception of the risks customers run by disclosing personal data via touchpoints under their control.*

H2b: *SME marketers' privacy literacy negatively affects the perception of the benefits customers can reap by disclosing personal data via touchpoints under their control.*

While privacy literacy is assumed to have a direct effect on the privacy orientation of touchpoints, it is also likely that this effect is partially mediated by a privacy calculus, as it is in customers' protective behaviour (see, e.g., Yun et al., 2019).

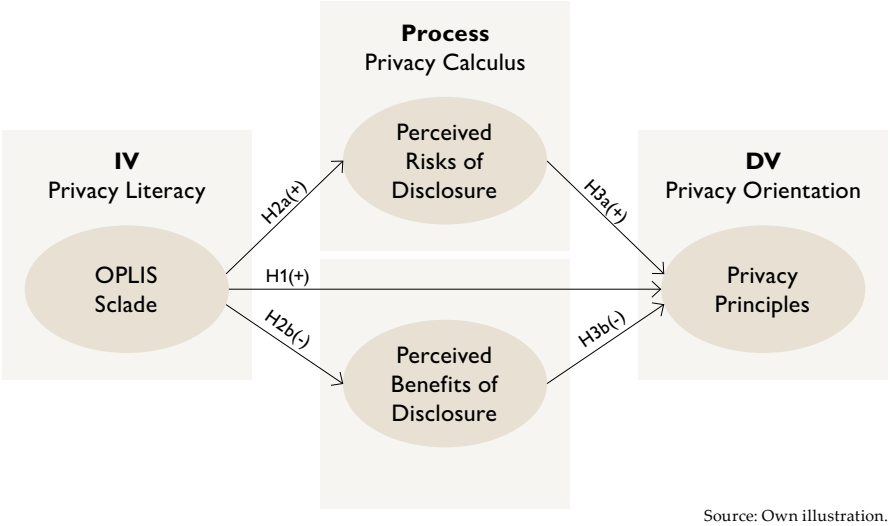
H3a: *SME marketers' perception of the risks customers run by disclosing personal data via touchpoints under their control positively influences the privacy orientation of said touchpoints.*

H3b: *SME marketers' perception of the benefits customers may reap by disclosing personal data via touchpoints under their control negatively influences the privacy orientation of said touchpoints.*

Methodology

The data were collected in two steps: first via an online survey targeted towards SME owners or employees with marketing responsibility and second by using a structured evaluation form for the corresponding websites and privacy policies. The data set was collected using direct mailings to SME marketers in Switzerland. A firm was defined as an SME if it employs less than 250 people (BFS, 2020). Additionally, all the SMEs in the sample had to operate within a business-to-consumer (B2C) context with access to their customers' personal data. The final sample came down to 55 SMEs operating a B2C business within Switzerland or Lichtenstein. Of those SMEs, almost 50% were microfirms (< 10 employees), approx. 40% were small firms (10-50 employees)

Figure 1: Hypotheses and Research Design



Source: Own illustration.

Management Summary

Marketers in small and medium-sized enterprises (SMEs) are able to promote firm-wide privacy measures by focusing their data needs and offering protection measures on the touchpoints under their control. Yet, to unlock this potential they need a basic level of know-how. Using survey data of 55 SMEs, a link between marketers' privacy literacy and their SMEs' privacy orientation was established. The results also show that most surveyed mar-keters do not exhibit a higher privacy literacy than the general public.

and about 10% were medium-sized companies (> 50 and < 250 employees).

The questionnaire the SMEs were sent consisted of two parts – the first one asking for demographics and measuring the calculus and various control variables (e.g., IT background). The second part, the Online Privacy Literacy Measurement Scale (OPLIS) developed by Trepte et al. (2015), was used to measure privacy literacy. The scale was developed on the basis of a qualitative content analysis of research articles and adapted for the German-speaking market (Masur et al., 2020). It was reduced by Masur et al. (2017, p. 256) to a 20-item validated scale, able to "predict the implementation of data protection measures".

To evaluate SMEs' privacy orientation, the evaluation method by Martin et al. (2017) was used. It treats SMEs' privacy policies as meaningful proxies for their actual privacy practices. Hence, for each SME, their privacy policies and their primary website were analysed. The evaluation was based on the legal requirements of the GDPR. The following aspects were taken into account:

(1) Provides support for exercising the right to object (opt-out options).
(2) Explains what kind of data are collected (type and scope of data collection).
(3) Explains how the collected data are used (purpose or use).
(4) Explains how these data will be shared in the course of exchange.
(5) Provides contact information for privacy inquiries.
(6) Informs about the use of cookies on the website.
(7) Informs about (or offers) the possibility to deactivate cookies.
(8) Informs whether and which analysis tools are used (e.g., Google Analytics).
(9) Gives information on users' rights, such as the right of information, deletion, correction and transfer of personal data.
(10) Deploys cookie banners on pages utilizing them.

The stricter requirements of the GDPR were applied to judge the Swiss SMEs' privacy policies, because it is assumed that the majority of data-collecting companies in Switzerland are affected by EU law due to the market location principle (see GDPR Art. 13, Ebert & Widmer, 2018; FDPIC, 2018; Möhle, 2021). We chose to sample Swiss SMEs because in general they demonstrate low expertise regarding GDPR guidelines although in principle they have to adopt them (Ebert & Widmer, 2018).

Results

The data of the 55 SMEs were compiled by one author and checked for accuracy (e.g., by re-reading privacy policies) as well as prepared for analysis by another. All data were compiled and analysed using IBM SPSS Statistics.

Privacy Literacy within SMEs

In order to put the overall privacy literacy of the SME participants in context, their results were compared to the norm table for privacy literacy within the general German population from the OPLIS guide created by Masur et al. (2020). It shows that the population average of 12 correctly answered questions was slightly but not significantly lower than the SME mean of 13.2. In total, only around 60% of SMEs demonstrated a privacy literacy above the population average. Unsurprisingly, the 11 SME participants with a background in IT exhibited a significantly higher ($p < 0.01$) mean OPLIS score than other participants.

OPLIS is designed to measure privacy literacy across four knowledge dimensions. Figure 2 shows the cumulative percentage of the knowledge levels across the dimensions within the sample. It shows that there are knowledge gaps relating to the data processing practices of third-party institutions (row 3) as well as the current legal practices (row 4). Both of these dimensions are critical in the assessment of potential risks of the disclosure of personal data (Masur et al., 2017), which might explain the gap in cyber security capabilities between SMEs and larger firms (Heidt et al., 2019; Van Haastrecht et al., 2021). These findings are also in line with previous studies which suggest that privacy literacy training is not regarded as highly important in SMEs (Ebert & Widmer, 2018; Heidt et al., 2019).

Lessons Learned

1 Since marketers in SMEs have more direct control over their firms' touchpoints, the level of their privacy literacy will help to determine the privacy orientation of these touchpoints.

2 Marketers with a higher privacy literacy will perceive a higher risk for customers to share personal data via their firm's website.

3 The privacy orientation of most SME websites will be geared towards the minimum legal requirements instead of the customers' potential privacy benefits.

4 Marketers with an academic or professional background in IT will exhibit a higher general privacy literacy.

5 A customer-oriented privacy policy implemented by SME marketers could help them exceed current privacy regulations while building the internal know-how and customer trust essential for the usage of data-intensive marketing technologies.

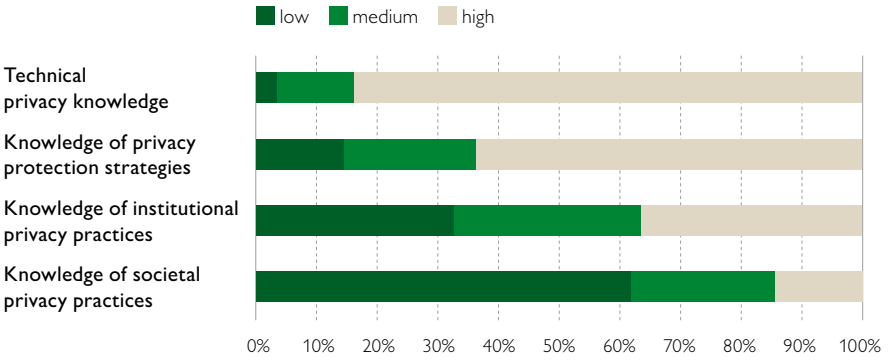
Website Privacy Orientation

The data on the privacy orientation of the SME websites were collected in a two-month period, directly after a participant had answered the questionnaire, and then reviewed to ensure a reliable reading. Figure 3 shows the individual percentages of requirements met by the SMEs.

The informational requirements (points 1 to 5) were met by the majority of SMEs in the sample (56%). SMEs usually informed customers that personal data would be collected, although it was not always specified exactly which data would be stored. When providing contact information for privacy inquiries, most of the SMEs listed their standard address (info@XYZ). This suggests that there is no specific office or person entrusted with this task and supports the assumption that SME marketers are able to exercise direct control over collected customer data.

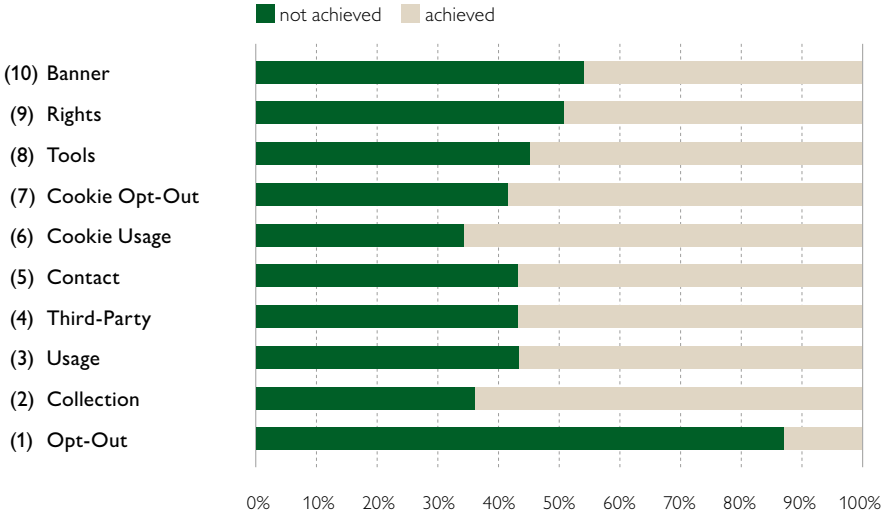
Overall, a majority of SMEs showed a medium to high privacy orientation on their website and with regard to their privacy policy, with 41.82% scoring 7–10 points (high), 18.18% scoring 5–6 points (medium), and 40% scoring 0–4 points (low). However, considering the measurement was derived from the minimum requirements found in the GDPR, SMEs are oriented towards minimal compliance only. Almost all privacy policies in the sample provide customers with some information on how data are collected, but without mentioning any specifics. This finding is in line with a larger shift in the "landscape of privacy policies" triggered by the ratification of the GDPR: coverage of privacy policies might have improved, but often at the cost of reduced specificity (Linden et al., 2020, p. 47).

Figure 2: OPLIS Knowledge Levels of the SME Participants



n=55. Source: Own illustration.

Figure 3: Website Privacy Orientation Items



n=55. Source: Own illustration.

The Connection Between Privacy Literacy and Privacy Orientation

The results show how privacy is understood and practiced within the SMEs in the sample, but it does not provide additional information on the relationship between the variables. Table 1 shows the correlations between all the variables in the proposed model.

Since several of the independent variables were found to be significantly correlated, the variance inflation factors were calculated to test for multicollinearity, but none of them exceeded the value of 2. While the focus was predominantly on testing the research model presented in figure 1, alternative models were also calculated to test the mediating effect of the privacy calculus, control for SME variables (e.g., industry) and interactions. However,

Table 1: Correlations Between the Model Variables

	OPLIS	Per. Risks	Per. Benefits	Privacy Orient.
OPLIS	1	.421**	.026	.313**
Per. Risks	.421**	1	.248*	.103
Per. Benefits	.026	.248*	1	-.151
Privacy Orient.	.313**	.103	-.151	1

* sign. at the 0.05 level (2-tailed) / ** sign. at the 0.01 level (2-tailed). Source: Own illustration.

these models did not show significant loadings (i.e., $p < .05$) and hence we proceeded to evaluate the original model's fit. Figure 4 shows the resulting path coefficients.

With $R^2 = .123$, the models' errors are only about 5% smaller on average than those of the constant-only model. The direction of the effects is as hypothesized, with privacy literacy increasing risk perception and privacy orientation, and the perception of benefits decreasing privacy orientation. However, only the first two paths showed a significant effect.

To test the effect on a group level, the sample was divided according to the OPLIS ranking suggested by Masur et al. (2020). Three groups were formed, with low (< 11 pt.), medium (12–15 pt.) and high OPLIS scores (> 15 pt.). While the mean value of privacy orientation of the medium group showed no significant difference to the others (5.2), in companies with a low privacy literacy the privacy orientation of the website (3.5) was found to be significantly lower than that of companies with a high privacy literacy (6.5). Despite the limited sample, this indicates that privacy literacy does affect the privacy orientation of SME touchpoints.

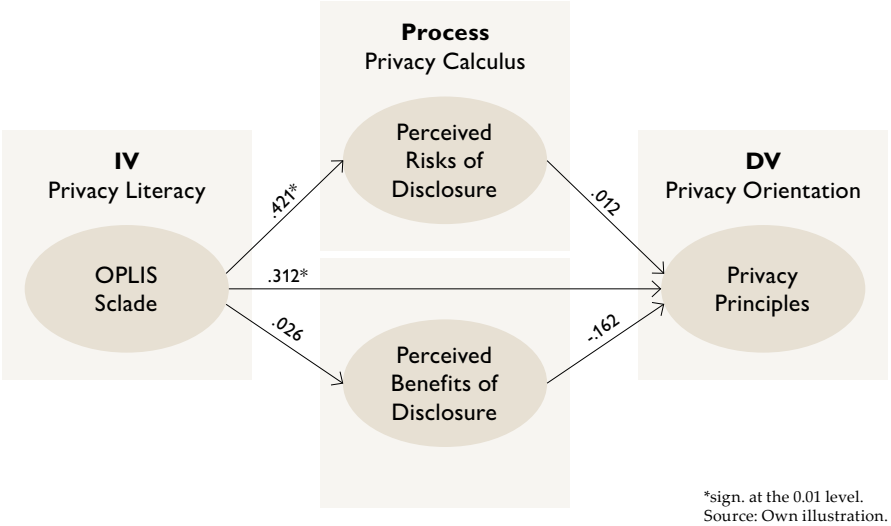
Discussion

We examined how the privacy literacy of SME marketers impacts their privacy calculus and the privacy orientation of the touchpoints under their control. By using a multiple regression approach and an analysis of variance, we were able to support the hypothesis that privacy literacy influences privacy orientation (H1 and H2a) but had to reject our proposed model regarding this relationship (H2b, H3a/b).

Though privacy literacy served as a significant predictor for the privacy orientation of the SMEs touchpoints, the privacy calculus could not be supported as the process used by marketers to translate knowledge into action. The fact that SME marketers with high privacy literacy rated the risks of disclosure higher than those with lower literacy while not adjusting privacy orientation based on their risk perception suggests that the decision to follow stricter privacy measures is not driven by a customer-centric logic. It is likely that the environmental context (e.g., less strict privacy laws in Switzerland), technical hurdles (e.g., out-of-the-box websites), and firm-specific considerations (e.g., marketing culture) have a larger influence than customer considerations (see also Sarathy & Robertson, 2003). Additionally, in line with the study by Ebert and Widmer (2018), Swiss SMEs do not seem to regard privacy as an important strategic mission.

The survey on privacy literacy showed that the knowledge level of SME marketers was only slightly above the population average. This indicates insufficient knowledge among SMEs regarding data protection and modern privacy practices – especially considering the generally low level of the OPLIS scale.

Figure 4: Model with Standardized Path Coefficients



*sign. at the 0.01 level.
Source: Own illustration.

The analysis of the websites and the data privacy statements showed that at least half of the SMEs only barely comply with current legal requirements. In every fifth firm, an explicit privacy policy was missing on the website. It can be assumed that many SMEs are still working with potentially problematic data. The majority of companies with a good data protection orientation met the basic requirements of the GDPR. However, the stricter provisions regarding the transparent use of customer data (e.g., what kind of user profiles are created based on sales data?) or the non-utilization of social media plugins (i.e., no usage of social network data for retargeting) were hardly met by any SME in the sample.

The hypothesis that higher privacy literacy leads to higher data protection orientation was supported. However, due to the comparatively low contribution of privacy literacy and the privacy calculus to data privacy orientation, considerations for the customers' view are unlikely to drive further privacy enhancements.

Lessons Learned

1. Marketers in SMEs show no more than average privacy literacy and about one in five of SME websites in the sample did not even feature an explicit privacy policy. This suggests a higher privacy risk when sharing customer data with SMEs.
2. Swiss SMEs should invest in meeting the GDPR's six basic principles – not just be-cause they have to, but because they represent a shift to a more customer-oriented privacy strategy.
3. Investing in privacy trainings for marketers could improve the privacy orientation of data collecting touchpoints and thus reduce legal and image risks.
4. Moving from a compliance-oriented towards a customer-oriented privacy strategy requires marketers with a high general privacy literacy.
5. Hiring marketers with an IT background is a short-term solution to raise the privacy literacy within a given firm.

Conclusion

Marketing strategies across industries are increasingly based on the processing of customer data. Along with these practices, privacy concerns in the population have increased (see, e.g., Auxier et al., 2019; Veritas, 2017). At the institutional level, companies are facing stricter legislation, with the introduction of the GDPR and the potential expansion of the nDSG in Switzerland (Pfister, 2021). Marketers, as key users of customer data, are thus increasingly caught in the conflict between the need for data processing and privacy protection.

In this context, this study researched whether the privacy literacy of SME marketers in a B2C context has an impact on the privacy orientation of their SME. The results show that the majority of SME marketers in the sample do not demonstrate a significantly higher privacy literacy than the general public. Additionally, almost half of the websites analysed did not implement all privacy measures demanded by the GDPR. Industry was no significant predictor of privacy orientation, but an IT background of the SME marketer was. While the privacy literacy of SME marketers served as a predictor of the implementation of privacy measures, it did not follow the logic of the privacy calculus. Hence, other factors not relating to the customers' potential risks and benefits drove the implementation of privacy measures within these SMEs. These results are in line with the previously reported reactive and compliance-oriented stance of SMEs when it comes to data privacy and cyber security (Ebert & Widmer, 2018; Heidt et al., 2019; Lopes & Melão, 2016; Van Haastrecht et al., 2021). Additionally, a qualitative finding in the analysis of the privacy statements was that they predominantly cited articles of law that are difficult to understand and that they were not communicatively oriented toward customers.

Since the privacy calculus does not seem to serve as a mediator between privacy literacy and privacy orientation, other process variables should be tested in future research. Examining an SME's structure, IT budget, data-processing practices or training efforts might produce a more complete understanding of how privacy literacy affects privacy orientation.

It is expected that SMEs will increasingly try to develop the capabilities to use big data applications to carve out a competitive advantage within their industries (Bianchini & Michalkova, 2019; Sen et al., 2016). However, their current privacy strategy that mainly focuses on compliance and self-management "cannot achieve the goals demanded of it" (Solove, 2013, p. 1903). Hence, a shift towards a more proactive privacy strategy – by investing early in the resources and the knowledge base to build privacy-compliant and secure data processes – is necessary to keep up with current privacy legislation and to meet the growing customer demand for privacy (Palmatier & Martin, 2019).

We have shown that marketers can contribute to the building of these resources and overall privacy orientation by acquiring a basic level of privacy literacy. Therefore, further investments in employee privacy trainings are a good start in the fight against privacy violations – after all, knowing the how and what of data privacy is half the battle.

Literature

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. Pre-Proceedings to EC'04, May 17–20, New York, 1–9.

Amiri, I., Wang, L., Levy, Y., & Hur, I. (2018). An empirical study on the factors contributing to disclosing personal information online: Insecurity in the digital age. Twenty-Fourth Americas Conference on Information Systems, 1–10.

Auxier, B. Y. B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019). Americans and privacy: Concerned, confused, and feeling a lack of control over their personal information. Pew Research Center, November, 1–63.

Barocas, S., & Nissenbaum, H. (2014). Computing ethics: Big data's end run around procedural privacy protections recognizing the inherent limitations of consent and anonymity. Communications of the ACM, 57(11), 31–33. https://doi.org/10.1145/2668897

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. Journal of Communication 67(1), 26–53. https://doi.org/10.1111/jcom.12276

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. Journal of Strategic Information Systems, 11, 245–270.

BFS. (2020, August 28). Kleine und mittlere Unternehmen. Bundesamt für Statistik. https://www.bfs.admin.ch/bfs/de/home/statistiken/industrie-dienstleistungen/unternehmen-beschaeftigte/wirtschaftsstruktur-unternehmen/kmu.html

Bianchini, M., & Michalkova, V. (2019). Data analytics in SMEs: Trends and policies. OECD SME and Entrepreneurship Papers, 15, 1–45. https://doi.org/10.1787/1de6c6a7-en

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2017). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, 34(3). https://doi.org/10.2307/25750690

Camra-Fierro, J., Centeno, E., Pérez-Cabañero, C., González-Cruz, T., & Cruz-Ros, S. (2012). Do family SME managers value marketing capabilities' contribution to firm performance? Marketing Intelligence & Planning 30(2), 116–142. https://doi.org/10.1108/02634501211211948

Coleman, S., Göb, R., Manco, G., Pievatolo, A., Tort-Martorell, X., & Reis, M. S. (2016). How can SMEs benefit from big data? Challenges and a path forward. Quality and Reliability Engineering International, 32(6), 2151–2164. https://doi.org/10.1002/QRE.2008

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for E-Commerce transactions. Information Systems Research, 17(1), 61–80. https://doi.org/10.1287/isre.1060.0080

Ebert, N., & Widmer, M. (2018). Datenschutz in Schweizer Unternehmen 2018. ZHAW Zürcher Hochschule für Angewandte Wissenschaften. https://doi.org/10.21256/ZHAW-4001

FDPIC. (2018). The GDPR and its consequences for Switzerland (Issue July). Federal Data Protection and Information Commissioner (FDPIC).

Gotsch, M. L., & Schögel, M. (2021). Addressing the privacy paradox on the organizational level: Review and future directions. Management Review Quarterly 2021, 1–34. https://doi.org/10.1007/S11301-021-00239-4

Heidt, M., Gerlach, J. P., & Buxmann, P. (2019). Investigating the security divide between SME and large companies: How SME characteristics influence organizational IT security investments. Information Systems Frontiers, 21(6), 1285–1305. https://doi.org/10.1007/S10796-019-09959-1

Hernández-Linares, R., Kellermanns, F. W., & López-Fernández, M. C. (2021). Dynamic capabilities and SME performance: The moderating effect of market orientation. Journal of Small Business Management, 59(1), 162–195. https://doi.org/10.1111/jsbm.12474

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers and Security, 64(November), 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Lekmat, L., Selvarajah, C., & Hewege, C. (2018). Relationship between market orientation, entrepreneurial orientation, and firm performance in thai SMEs: The mediating role of marketing capabilities. International Journal of Business and Economics, 17(3), 213–237

Linden, T., Khandelwal, R., Harkous, H., & Fawaz, K. (2020). The privacy policy landscape after the GDPR. Proceedings on Privacy Enhancing Technologies, 1, 47–64. https://doi.org/10.2478/popets-2020-0004

Lopes, L. A., & Melão, N. F. (2016). Website content and design in SME: Insights from Portugal. International Journal of Electronic Business, 13(1), 70–97. https://doi.org/10.1504/IJEB.2016.075343

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. Journal of Marketing, 81(1), 36–58. https://doi.org/10.1509/jm.15.0497

Masur, P. K., Teutsch, D., & Trepte, S. (2017). Entwicklung und Validierung der Online-Privatheits-kompetenzskala (OPLIS). Diagnostica, 63(4), 256–268. https://doi.org/10.1026/0012-1924/A000179

Masur, P. K., Teutsch, D., & Trepte, S. (2020). OPLIS Manual. Universität Hohenheim.

Möhle, J.-P. (2021). Totalrevision des Schweizer Datenschutzgesetzes – Ende gut, alles gut? Datenschutz und Datensicherheit, 45(9), 598–602. https://doi.org/10.1007/S11623-021-1498-Y

Nissenbaum, H. (2010). Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press.

Norberg, P. A., & Horne, D. R. (2007). Privacy attitudes and privacy-related behavior. Psychology & Marketing, 24(10), 829–847. https://doi.org/10.1002/mar.20186

Palmatier, R. W., & Martin, K. D. (2019). The Intelligent Marketer's Guide to Data Privacy. Palgrave Macmillan.

Parker, R. B. (1974). A definition of privacy. Rutgers Law Review, 27(2), 275–297.

Petronio, S. (2010). Communication privacy management theory: What do we know about family privacy regulation? Journal of Family Theory & Review, 2(3), 175–196. https://doi.org/10.1111/j.1756-2589.2010.00052.x

Pfister, W. (2021). «Für KMU ist es von Vorteil, sich auf das neue Datenschutzgesetz vorzubereiten». KMU Portal, WBF: Eidgenössisches Departement für Wirtschaft, Bildung und Forschung. https://www.kmu.admin.ch/kmu/de/home/aktuell/interviews/2021/fuer-kmu-ist-es-von-vorteil-sich-auf-das-neue-datenschutzgesetz-vorzubereiten.html

Sarathy, R., & Robertson, C. J. (2003). Strategic and ethical considerations in managing digital privacy. Journal of Business Ethics, 46(2), 111–126.

Schögel, M. (2016). Marketing automation, machine learning und artificial intelligence. Marketing Review St. Gallen, 33(4), 3–5.

Sen, D., Ozturk, M., & Vayvay, O. (2016). An overview of big data for growth in SMEs. Procedia – Social and Behavioral Sciences, 235, 159–167. https://doi.org/10.1016/J.SBSPRO.2016.11.011

Solove, D. J. (2013). Privacy self-management and the consent dilemma. Harvard Law Review, 126, 1880–1903.

Solove, D. J. (2021). The myth of the privacy paradox. George Washington Law Review, 89(1), 1–51.

Stuart, T. (2021). Too little too late? An exploration and analysis of the inadequacies of anti-trust law when regulating GAFAM data-driven mergers and the potential legal remedies available in the age of Big Data. European Competition Journal, 17(2), 407–436. https://doi.org/10.1080/17441056.2021.1909234

Taneja, A., Vitrano, J., & Gengo, N. J. (2014). Rationality-based beliefs affecting individual's attitude and intention to use privacy controls on Facebook: An empirical investigation. Computers in Human Behavior, 38, 159–173. https://doi.org/10.1016/j.chb.2014.05.027

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do people know about privacy and data protection strategies? Towards the "Online Privacy Literacy Scale" (OPLIS). In S. Gutwirth, R. Leenes, & P. de Hert (Eds.), Reforming European data protection law (pp. 333–365). Springer. https://doi.org/10.1007/978-94-017-9385-8_14

Van Haastrecht, M., Sarhan, I., Shojaifar, A., Baumgartner, L., Mallouli, W., & Spruit, M. (2021). A threat-based cybersecurity risk assessment approach addressing SME needs. ACM International Conference Proceeding Series, 1–12. https://doi.org/10.1145/3465481.3469199

Veritas. (2017). 2017 Veritas Gdpr Report. Veritas Schweiz AG.

Yun, H., Lee, G., & Kim, D. J. (2019). A chronological review of empirical research on personal information privacy concerns: An analysis of contexts and research constructs. Information and Management, 56(4), 570–601. https://doi.org/10.1016/j.im.2018.10.001

Zhu, H., Ou, C. X. J., Van den Heuvel, W. J. A. M., & Liu, H. (2017). Privacy calculus and its utility for personalization services in e-commerce: An analysis of consumer decision-making. Information & Management, 54(4), 427–437. https://doi.org/10.1016/j.im.2016.10.001

Zuboff, S. (2019). Surveillance capitalism and the challenge of collective cction. New Labor Forum, 28(1), 10–29. https://doi.org/10.1177/1095796018819461