



## Online Customer Trust in the Context of the General Data Protection Regulation (GDPR)

Jingjing Zhang<sup>1,\*</sup>, Farkhondeh Hassandoust<sup>2</sup>, Jocelyn E. Williams<sup>3</sup>

<sup>1</sup>New Zealand, [jzh1616@gmail.com](mailto:jzh1616@gmail.com)

<sup>2</sup>Auckland University of Technology, New Zealand, [fhassand@aut.ac.nz](mailto:fhassand@aut.ac.nz)

<sup>3</sup>ICL Graduate Business School, New Zealand, [jocelynwilliams@icl.ac.nz](mailto:jocelynwilliams@icl.ac.nz)

### Abstract

**Background:** A recent global survey found that almost half of Internet users who never buy online indicated lack of trust as the main reason. The General Data Protection Regulation (GDPR) is new legislation expected to provide the opportunity for organizations to improve their customer trust through personal data governance. Few studies explore online customer trust from the GDPR perspective. This study aims to fill this gap by drawing on the Technology Acceptance Model (TAM) and Self-Determination Theory (SDT), examining the antecedents of online customer trust from the GDPR perspective. The study also attempts to derive insights about the GDPR that may affect online customer trust, but which to date have little presence in frameworks of the antecedents of online trust. The main research questions are as follows. First, what are the impacts of perceived technology, perceived risks and perceived trustworthiness on online customer trust in the GDPR context? Second, what are the GDPR-specific factors that may affect online customer trust?

**Method:** This positivist study used a survey strategy with a deductive approach to investigate the research questions. A questionnaire was designed for primary data collection as the basis for quantitative data analysis.

**Results:** Data analysis confirmed that several GDPR-related trust antecedents – perceived security, perceived third-party assurance and perceived openness – are positively associated with online customer trust. This study offers new insights into the SDT adaptation that suggest the value of motivation theory for trust research in the GDPR context. This study also generates insights about the GDPR that may affect online customer trust.

**Conclusions:** This study suggests that the GDPR plays a significant role in online customer trust by bringing about stronger rights and more transparency for online customers. Both the confirmation and insights are a contribution that can lead seemingly old-fashioned trust antecedents into a new application.

**Keywords:** online customer trust, the General Data Protection Regulation (GDPR), the Technology Acceptance Model (TAM), the Self-Determination Theory (SDT).

Citation: Zhang, J., Hassandoust, F., & Williams, J. E. (2020). Online Customer Trust in the Context of the General Data Protection Regulation (GDPR). *Pacific Asia Journal of the Association for Information Systems*, 12(1), 86-122. <https://doi.org/10.17705/1pais.12104>  
Copyright © Association for Information Systems.

## Introduction

*The private information of tens of millions of Facebook users was collected by Cambridge Analytica without users' consent (Kuhn, 2018). Facebook's CEO Mark Zuckerberg admitted that it was "a breach of trust between Facebook and the people" (Forbes.com, 2019b). Facebook could have been fined up to \$1.8 billion, after the adoption of the General Data Protection Regulation (GDPR) (Forbes.com, 2019a).*

All major institutions globally, including business, government, non-governmental agencies (NGOs) and the media, have experienced significant decreases in trust since the mid-1960s (Clark et al., 2017). In line with this trend, a recent survey on global Internet trust and security found that among those respondents who never shop online, 49% indicated a lack of trust as the main reason why they refrained from making online purchases. The survey also found that Internet companies are one of the top three sources of privacy concern for customers, along with cybercriminals and governments (Centre for International Governance Innovation, 2019). Several researchers have also raised lack of trust as a significant reason why customers do not buy from online retailers (e.g., Grabner-Kräuter & Kaluscha, 2003; Kim et al., 2016; Oliveira et al., 2017; Ribbink et al., 2004). Yet trust is essential in all areas of a functioning society including the business world. Here it plays a powerful role in promoting successful relationships that enhance the business, reducing risk and uncertainty, and increasing willingness to purchase (Chang & Fang, 2013). Likewise, online customers' trust may lead to buying behavior in Internet transactions as a result, and it has a predominant influence on customers' online purchase intention (Chen & Barnes, 2007). Meanwhile, in the e-commerce context, the significance of online trust is heightened also because of the high degree of risk and uncertainty inherent in most online transactions (Pavlou, 2003). If customer trust is eroded, it could result in an unwillingness to purchase online, and website-based retailers may thus face a severe challenge to rebuild that trust (Wang & Emurian, 2005). For these reasons, and given the dramatic growth in online consumer spending, there is an urgent need to explore online customer trust, especially the antecedents that significantly affect it, and to investigate if there is a relationship between online customer trust and purchase intention.

European authorities assert that users' lack of trust in privacy standards is the major obstacle to both the application of digital services and the progress of the European Union's (EU) digital economy (Ciriani, 2015). Thus the EU has established the GDPR, a law to improve European users' data privacy (Boban, 2018b; Ciriani, 2015) and to ensure they have trust when sharing personal data. Approved by the European Parliament in 2016 (EUR-Lex, 2019) with full effect from May 2018 (Boban, 2018a), this law is expected to increase user trust, transparency and accountability of online processes, as well as influence the legal frameworks of other non-EU countries (Addis & Kutar, 2018). In light of economic globalization, most firms with a global span of operations must comply with the GDPR (Bandyopadhyay & Bandyopadhyay, 2018). Companies such as Facebook have proposed a cost-saving strategy that extends the GDPR protections to all customers if they opt-in (Menon, 2019). An impact of the GDPR on global technology development associated with cybersecurity and privacy protection has been identified (e.g., Li et al., 2019; Menon, 2019). Against this background, all customers, including both EU and non-EU citizens, can benefit from GDPR compliance. The GDPR context extends beyond the existing e-commerce research in terms of online trust, to aspects like the extensive jurisdictional reach of the regulation (Goddard, 2017). Few trust-related studies explore the unique context of the privacy policies and regulations or investigate perceived technology, perceived risks and perceived trustworthiness in an integrated conceptual model. Therefore, a theoretical gap exists between extant literature and the present study in the GDPR context, which creates the research motivations of this study. It is timely to conduct research on trust-based improvements from the GDPR perspective with respect to all customers regardless of their nationality or location. Because few studies have focused on this topic, this research is likely to add insights to existing studies on online customer trust. The main purpose of the present study is to fill this gap by drawing on the Technology Acceptance Model (TAM) (Davis,

1989) and Self-Determination Theory (SDT) (Deci & Ryan, 2008), examining the antecedents of online customer trust from the GDPR perspective. The study also attempts to derive insights about the GDPR that may affect online customer trust, but which to date have little presence in frameworks of its antecedents.

TAM is one of the most robust and concise frameworks for explaining the acceptance of online shopping by customers (Çelik, 2011; Koufaris & Hampton-Sosa, 2004; Reimers et al., 2016). SDT is an empirical approach to people's motivation that investigates their innate growth tendencies and psychological needs on the basis of self-motivation and personality (Ryan & Deci, 2000). Following TAM, the present study adopts perceived usefulness and perceived ease-of-use as trust antecedents to measure online customer trust that could in turn affect online purchase intention. Motivation theory has been a stream of information systems (IS) research that aims to explain factors affecting technology acceptance (Akhlaq & Ahmed, 2013; Fagan et al., 2008). The present research also applies SDT, especially its extrinsic motivation type, as part of the theoretical foundation to investigate determinant factors towards external events on customers' trust attitude. Based on SDT, the constructs including perceived privacy, perceived security and perceived third-party assurance are selected as most significant extrinsic motivations for online customer trust and are proposed in the research model.

The main research questions derived from the above research purpose are as follows. First, what are the impacts of the perceived technology, perceived risks and perceived trustworthiness on online customer trust in the GDPR context? Second, what are the GDPR-specific factors that may affect online customer trust? This paper begins with a literature review on online customer trust and the GDPR as a basis for our research model and hypotheses. An overview of the research design and methods is presented, followed by data analysis and findings that inform discussion. Some theoretical and practical contributions of the study are identified as well as limitations and future research directions.

## Literature Review

### Trust

Trust is a crucial relationship concept that has various definitions from different disciplinary perspectives (Chang & Fang, 2013; Lewicki & Bunker, 1995; McKnight & Chervany, 2001). A widely-acknowledged definition of trust is "a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another" (Rousseau et al., 1998, p.395). Online customer trust is essential for creating expected and satisfied outcomes in Internet transactions (Chen & Barnes, 2007), and it shows a favorable influence on customers' online purchase intention (Jarvenpaa et al., 2000; Pavlou, 2003). Research has shown that high levels of customers' online trust encourage their purchase intention and help ensure their repeat custom (Gefen & Straub, 2004). On the other hand, a human being in the online environment has to trust in a man-made object instead of another human being (Bauman, 2015). Thus, when customers conduct activities on a specific informational or transactional website, their trust would be "an attitude of confident expectation in an online situation of risk that one's vulnerabilities will not be exploited" (Corritore et al., 2003, p.740).

Different dimensions and types of trust have been developed (Das & Teng, 2004). For example, Mayer et al. (1995) created a model showing trust dimensions that includes the perception of trustors towards the trustees' benevolence, ability and integrity. McKnight and Chervany (2001) proposed an interdisciplinary model of high-level trust concepts, where trust is related to online consumer behaviors and has three dimensions. These are: dispositional trust (from psychology), institution-based trust (from sociology), and interpersonal trust (from social psychology). All of these can also be categorized into subjective trust (trust as a

perception), trust antecedents (various situational and personal factors that result in subjective trust), and behavioral trust (the actions arising from subjective trust) (Das & Teng, 2004). Trust antecedents serve as signals that moderate trust between customers and retailers (Belanger et al., 2002; Xiao et al., 2016). They are related to various situational and personal factors that cause subjective trust (Das & Teng, 2004). Likewise, the antecedents of online customer trust can be understood as determinant factors that create the conditions for trust to online customers.

Antecedents of online customer trust can be grouped into three major categories: customer-based, website-based and organization-based (Beldad et al., 2010; Chen & Dhillon, 2003). Previous studies have investigated numerous antecedents of online customer trust such as website reliability, responsiveness, (Kim et al., 2009), online security and privacy (Kim et al., 2009; Köksal & Penez, 2015), consumer reviews, and e-commerce experience (Köksal & Penez, 2015). Online customer trust has also been identified to have six determinant factors including technology, presentation, security assurance, brand (reputation), fulfilment (willingness to customize to meet personal demands), and interactions (Chen & Barnes, 2007; Yoon, 2002). Subsequently, these factors can be classified into three main aspects: perceived technology, perceived risks and company competency [or perceived trustworthiness] (Chen & Barnes, 2007). Perceived technology and perceived risks are aspects related to website-based perceptions (Koufaris & Hampton-Sosa, 2004). In our research, company competency is replaced by perceived trustworthiness, because we infer perceived trustworthiness incorporates the concept of company competency and it offers more sources for further investigation. Perceived trustworthiness pertains to organizational-based perceptions.

### **Perceived technology**

Useful, comprehensible information on websites can increase the level of online customer trust, reduce information asymmetry, and positively influence purchase intention (Koufaris & Hampton-Sosa, 2004). Davis (1989) proposes that a potential customer's attitude towards using a given system is a function of two beliefs – perceived usefulness and perceived ease-of-use. Perceived usefulness and perceived ease-of-use determine a user's intention to willingly accept the new information technology (IT) (Gefen et al., 2003a). They can be understood as two key perceptions of technology that cause people to reject or accept the new IT-based system. Numerous studies have confirmed that perceived usefulness and perceived ease-of-use significantly affect user attitudes, which have an impact on user adoption of an IT-based system (Amin et al., 2014). Perceived usefulness is defined as the extent to which people believe that using a specific system would improve their job performance (Davis, 1989). In the online buying context, perceived usefulness refers to the extent to which customers believe that using a website as a medium would enhance their job performance (Chen & Barnes, 2007; Cho & Sagynov, 2015; Van der Heijden et al., 2003), and benevolence toward the website (Chen & Barnes, 2007). Perceived ease-of-use is defined as the extent to which people believe that using a specific system would be effortless (Davis, 1989). In the online context, perceived ease-of-use refers to customers' perceptions that purchasing on the Internet would involve a minimum amount of effort. In summary, perceived usefulness is the degree to which purchasing online [from a website] is effective in assisting customers to complete their tasks, while perceived ease-of-use is how easy the Internet [a website] is to use as a trading medium (Cho & Sagynov, 2015; Monsuwé et al., 2004).

### **Perceived risks**

In a purchase situation, perceived risks refer to the fundamental uncertainty about the purchase outcomes and the significance of the consequences of making an incorrect choice (Chen & Barnes, 2007; Hunter et al., 2004). Trust is not taking a risk but is a willingness to accept a risk (Mayer et al., 1995). Risk and trust are interactive, and some degree of risk will always exist when a person trusts something (Chang et al., 2016). In the IS field, perceived



risks are pertinent to the potential for loss when customers use digital services (Pavlou, 2003). Customers are most concerned about online security and privacy when they shop online (Chang et al., 2016). Many studies indicate that improved online customer trust could effectively reduce customers' perception of risk in shopping online (Chang et al., 2016; Lee & Turban, 2001; McKnight & Chervany, 2001). Websites could reduce those risks in the Internet environment by enhancing features related to security and privacy (Chen & Barnes, 2007).

*Perceived privacy, perceived security and perceived third-party assurance* are three key elements of trust antecedents which address perceived risks and improve online customer trust (Bojang, 2017; Chen & Barnes, 2007; Davis et al., 2011; Mukherjee & Nath, 2007). Perceived privacy refers to the ability of customers to control their information with no interference from external individuals or bodies (Bojang, 2017). In the privacy context, trust refers to consumers' expectations that online retailers will ensure their information will be treated fairly or without bias (Bojang, 2017). Previous studies stress the importance of information privacy as a decisive factor in online customer trust (Petrovic et al., 2003, as cited in Bojang, 2017).

Perceived security of a website refers to the feeling of safety when they use the computer and share their financial information online (Bart et al., 2005; Mukherjee & Nath, 2007). Perceived security also refers to people's subjective judgement about the likelihood that their sensitive information would not be seen, stored or controlled by inappropriate parties during the storage or transit process, and in a method consistent with their positive expectations (Ong & Lin, 2015). Empirical research asserts that perceived security is positively associated with trust in e-commerce contexts (e.g., Bojang, 2017; Mukherjee & Nath, 2007).

Perceived third-party assurance is another significant factor in explaining online customer trust (Bojang, 2017; Greenberg et al., 2008). Third-party assurance refers to organizations that act as assurers who confirm to customers that a specific retailer follows the rules made by the assurer (Davis et al., 2011). Various e-commerce services from third-party organizations have appeared to facilitate trust between online retailers and customers. Retailers willing to achieve a third-party assurer's standards, adopt a third-party certified technology, or agree to abide by the assurer's procedures are permitted by assurers to show an assurance seal or identifying logo (Kimery & McCord, 2002). Customers are more likely to trust those online retailers who make efforts such as presenting third-party assurance seals (Wu et al., 2010). Certifications from trusted third parties can compensate for an online retailer's lack of transactional history with its customer (Beldad et al., 2010; Koehn, 2003). For instance, ISO certifications such as ISO 9001 are used effectively to establish trust between enterprises and customers, and are viewed as an external motivating factor to satisfy customer expectations (Kaziliunas, 2010).

### ***Perceived trustworthiness***

Trustworthiness is one characteristic of the trustee. *Perceived trustworthiness* is the perception of how trustworthy the trustee is (Gefen et al., 2003b; Mayer et al., 1995). If a trustee obtains something by lying, s/he would be regarded as being less trustworthy (Mayer et al., 1995). In the online context, a retailer will lose its customers when it is not considered trustworthy (Mou & Cohen, 2015). Extant literature suggests that one has to be trustworthy in order to build trust (Yu et al., 2015), while perceived trustworthiness has been found to have a significant impact on the continuance of trust (Liao et al., 2009). For example, when clients perceive Internet banking as trustworthy, they are able to extend their trust in it (Zhu & Chen, 2012). Moreover, perceived trustworthiness has been recognized as a critical factor in stimulating business transactions over the Internet (Liao et al., 2009).

Perceived trustworthiness is widely seen to have different attributes (or dimensions). Butler (1991) identifies five attributes of trustworthiness ranked in order of importance: competence, integrity, consistency, loyalty and openness. Openness refers to freely sharing information

and ideas (Butler, 1991), which is interpreted as website transparency and website interactivity in the online context (Kim et al, 2014; La Porte et al., 2002). Perceived openness could be a strategic method to build public trust in organizations (Kim et al., 2014). The degree to which a website can improve its openness of information will affect the ability of the website to meet online customers' demands (Mukherjee & Nath, 2003). Transparency means ensuring everything is visible, denoting one's openness or open communication to pursue trustworthiness (Kim et al., 2014). Numerous researchers discuss transparency in terms of a firm's openness about sharing information, and transparency can be conceptualized as openness within firms (Parris et al., 2016). When transparency is defined as openness of information, transparency and openness could be used in an interchangeable way.

### **Online purchase intention**

*Online purchase intention* is defined as a point when a customer has the willingness and intention to be engaged in online transactions (Chen & Barnes, 2007; Pavlou, 2003). Following the theory of reasoned action from Fishbein and Ajzen (1975), a customer's intention to purchase is preceded by the customer's attitude towards the purchase (Jarvenpaa et al., 2000). Attitude is directly affected by beliefs, and the higher the level of trust, the more favorable the attitude (Hsu et al., 2014; Jarvenpaa et al., 2000). Research has shown that online customer trust positively influences Internet-based purchase intention (Gefen & Straub, 2004; Pavlou, 2003; Singh & Matsui, 2017; Yoon, 2002). Trust makes online customers comfortable to share their information, perform transactions, and act upon advice from websites. These behaviors are all essential to extensive use of e-commerce (Bianchi & Andrews, 2012). Taking it a step further, trust eases behavioral uncertainty associated with the retailer, providing customers with a perception of control over a potentially risky purchase. Consequently, customers' sense of entire control over Internet transactions has a positive relationship with online purchase intentions (Pavlou, 2003).

### **The General Data Protection Regulation**

The GDPR is a new law "designed to harmonize data privacy laws across [the] EU, to protect and empower all EU citizens' data privacy and to reshape the way organizations across the EU approach data privacy" (European Commission, 2019b, p.5). Its chief aim is to strengthen EU citizens' control of their own data and to simplify the business regulatory environment (Zunko, 2017). The GDPR is focused on privacy and security laws (Ciriani, 2015) and regulates the processing by a company, an organization, or an individual, of personal data relevant to individuals in the EU (European Commission, 2019e). It has established a new suite of standardized rules regarding consumer data protection with several general principles of data protection – fairness, lawfulness and transparency, data minimization, purpose limitation, storage limitation, accuracy, as well as confidentiality and integrity (Bandyopadhyay & Bandyopadhyay, 2018; European Commission, 2019d; Goddard, 2017).

The GDPR is designed to ensure EU citizens have trust when providing their personal data (Boban, 2018a). It also indicates that creating trust is important as it allows the development of the digital economy in the EU market (EUR-Lex, 2019). Therefore, the GDPR can be considered to have a natural relationship to online customer trust in the digital age. It is further expected to create the opportunity for organizations to improve their customer trust through risk-related personal data governance (European Commission, 2019c; Wachter, 2018). The European Commission anticipates that the GDPR will bring major improvements in addressing future data-protection violations: clear language, stronger rights, more transparency, consent from users, and stronger enforcement. The improvements are explained in Table 1 and more information about the improvements is shown in Appendix A, based on a review of an introductory document (see Appendix B), legal articles and academic sources. Several features common to both the GDPR studies and studies of the antecedents of online customer trust have been identified: clear language with perceived usefulness and ease-of-use; stronger

rights with perceived privacy, perceived security, and perceived third-party assurance; and more information transparency with perceived openness (European Commission, 2019a). It may be inferred that the GDPR could play a role in those antecedents of online customer trust, particularly through its features of clear language, stronger rights and more information transparency.

**Table 1 - Five Improvements Brought from the GDPR**

Improvement	Explanation
Clear language	Privacy policies of organizations are to be written in a straightforward and clear language.
Stronger rights	Users have to be informed by organizations without delay in the event of harmful personal data breach, (e.g., if the data are stolen); Users can move their data to another competing service (e.g., to another platform of social media); Users have the right to access and have a copy of their data that organizations keep; Users hold a clearly defined “right to erasure” or “right to be forgotten” with well-defined safeguards.
More transparency	Organizations have to clearly inform users when transferring their data outside the EU; Organizations have to collect and process personal data only for a clear purpose, and they must inform users about new purposes if they are different from the purpose initially announced for data processing; Organizations have to inform users if the decision is automated and offer them the opportunity to dispute it.
Consent from the user	An affirmative consent needs to be given by users before their data can be used by organizations; Silence no longer means consent.
Stronger enforcement	Twenty-eight data protection authorities, grouped by the European Data Protection Board, exercise the power to offer guidance and interpretation, and use binding decisions in the case of multiple EU countries with respect to the same case; The authorities enjoy harmonized powers and impose fines on organizations to a maximum of €20 million or four per cent of worldwide annual turnover.

*Note: Adapted from European Commission (2019a), see also Appendix B.*

The GDPR includes 99 articles that comprise (data protection) principles, rights of the data subject (residents), controller and processor, transfers of personal data to third countries or international organizations, remedies, and liability and penalties among others (EUR-Lex, 2019). Despite a focus on EU citizens, the GDPR would be beneficial to non-EU customers through such elements as the principles relating to processing of personal data in Article 5, lawfulness of processing in Article 6 and the security of processing in Article 32. Jurisdiction based uniquely on the territoriality principle is less evident in the digital era (De Hert & Czerniawski, 2016). The extensive jurisdictional reach of the GDPR implies that in a universally connected global economy, almost any firm with an international operational reach will have to comply with the GDPR (Bandyopadhyay & Bandyopadhyay, 2018). It can be understood that, when companies have a high standard concerning privacy, security and third-parties (GDPR compliance), they treat customers in the same way due to the costs involved, especially in terms of the processing of customers’ personal data, the lawfulness of data processing and the security of processing. Thus, regardless of nationality or location, any customer is eventually considered to benefit from the rights and compliances of the GDPR.

### ***The Technology Acceptance Model (TAM)***

TAM (Davis, 1989) is one of the most commonly utilized models in IT adoption research (Gefen & Straub, 2000), and has proved to be appropriate as a theoretical foundation for e-commerce adoption by many researchers (e.g., Hassanein & Head, 2007; Kim, 2012; Moon & Kim, 2001). In TAM, the two constructs of perceived usefulness and perceived ease-of-use are identified as having a significant correlation with users' acceptance of IS (Davis, 1989). TAM is built on the theory of reasoned action and is concerned with the determinants of consciously intended behaviors (Davis et al., 1989; Fishbein & Ajzen, 1975; Pikkarainen et al., 2004). A well-designed website that is both useful and easy-to-use can be viewed as proof of the retailer's capabilities (Koufaris & Hampton-Sosa, 2004). The belief that retailers have the capabilities and resources to fulfil their promises is crucial in developing customer trust (Chow & Holden, 1997; Koufaris & Hampton-Sosa, 2004). In turn, useful, easily understood information on websites is thought to increase the degree of online customer trust (Chen & Barnes, 2007; Koufaris & Hampton-Sosa, 2004). Grounded in TAM, the present study adopts perceived usefulness and perceived ease-of-use as two variables of trust antecedents, and examines their impacts on online customer trust in the context of the GDPR. In addition, TAM is partially used to explain elements influencing online customer trust and online purchase intention in existing studies (e.g., Chen & Barnes 2007; Cho & Sagynov, 2015; Gefen et al., 2003a; Roca et al., 2009; Van der Heijden et al., 2003). Thus, our research adopts TAM to explain the relationship between customers' trust and their buying intention in the online context.

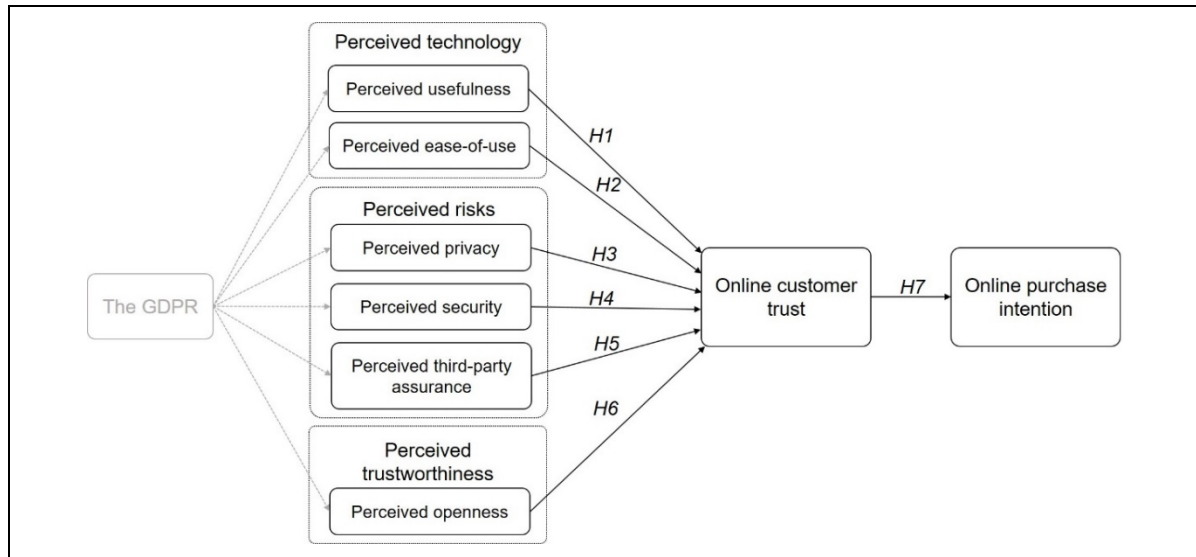
### ***The Self-Determination Theory (SDT)***

All human behaviors are generated by a series of motivations (Chang et al., 2016; Deci & Ryan, 1985). SDT, an empirical approach to people's motivation and personality (Ryan & Deci, 2000), has been used as a critical framework to assess the motivation and satisfaction of customers (Kumar et al., 2018). This theory particularly focuses on explaining types of motivation (Deci & Ryan, 2008), and has been adopted in IS research to explore the factors that impact IS acceptance (Fagan et al., 2008; French, 2017; Wu & Lu, 2013). In SDT, motivation consists of extrinsic motivation and intrinsic motivation depending on the extent of self-determination (Chang et al., 2016; Ryan & Deci, 2000; Wu & Lu, 2013). Both intrinsic and extrinsic motivations determine whether people engage in certain actions (Chang et al., 2016). Intrinsic motivation refers to performing an action for the inherent interest, enjoyment, or satisfaction of the action itself (Chang et al., 2016; Ryan & Deci, 2000). Extrinsic motivation refers to performing an action in order to obtain [or avoid] some separable consequences. It is pertinent to the effect of external events on people's motivation (Ryan & Deci, 2000) that can be either positive such as a prize (Wu & Lu, 2013) or negative from pressures such as threats of punishment (Deci et al., 1991; Ryan & Deci, 2000). In the context of existing research on online customer trust, security and privacy provided by websites are regarded as extrinsic motivation that affect customers' trust and further purchase intention behavior (e.g., Chang et al., 2016; Chen & Barnes, 2007). Furthermore, third parties have become the most significant way to motivate customers to engage in online activities (Pavlou et al., 2003; Salo & Karjaluoto, 2007). Thus, the present study regards perceived privacy, perceived security, and perceived third-party assurance as external sources that extrinsically motivate online customer trust and reduce customer-perceived risk of shopping online.



## Research Model and Hypotheses

Based on the previous theoretical discussion, this study proposes the research model in Figure 1. This model comprises eight constructs identified from the literature review. Perceived usefulness, perceived ease-of-use, perceived privacy, perceived security, perceived third-party assurance, as well as perceived openness are hypothesized as the antecedents of online customer trust. The model presumes a relationship between online customer trust and online purchase intention.



**Figure 1 - A Conceptual Model**

Useful and easily comprehended website information can increase the level of online customer trust, reduce asymmetric information, and positively influence purchase intention (Koufaris & Hampton-Sosa, 2004). Perceived usefulness and perceived ease-of-use are two main belief variables of TAM (Koufaris & Hampton-Sosa, 2004), which are thought to have a significant influence on attitude (Koufaris, 2002; Reimers et al., 2016), trust (Roca et al., 2009), or initial trust in the e-commerce context (Koufaris & Hampton-Sosa, 2004). These factors are used to explain the antecedents affecting online customer trust and online purchase intention of customers (Chen & Barnes, 2007; Gefen et al., 2003a; and Van der Heijden et al., 2003). Customers may adopt a particular system if they believe it will bring benefits such as improving shopping efficiency; also, if customers feel that an online service is easy to handle and free of effort, the likelihood that they will use the system may be higher (Chong et al., 2010). A clear language regulation from the GDPR requires organizations to provide information in a concise, effortlessly accessible form by using plain and clear language, which is likely related to perceived usefulness and ease-of-use of the websites of retailers. Thus, two hypotheses are proposed as follows:

*H1. The perceived usefulness of a website is positively associated with online customer trust.*

*H2. The perceived ease-of-use of a website is positively associated with online customer trust.*

Motivation theory has a significant impact on both behavior and behavioral intention across many studies (Vallerand, 1997). Drawing on SDT, perceived privacy, perceived security and perceived third-party assurance are modeled as three extrinsically motivational factors, that are associated with the impact of external resources on people's motivation. Moreover, the well-defined safeguards and supervisory authority brought by the GDPR and set up by member states (Voss, 2017) enhance customers' rights to data privacy (European Commission, 2019a). Thus, the GDPR's emphasis on stronger rights is associated with

individuals' perceptions of privacy, security and third-party assurance. Perceived privacy and perceived security are expected to be trust antecedents dealing with perceived risks and improving online customer trust in many studies (Bojang, 2017; Chen & Barnes, 2007; Davis et al., 2011; Mukherjee & Nath, 2007). In an e-commerce context, privacy and security concerns are the major reason customers do not buy products from websites (Gurung & Raja, 2016). To address these concerns, websites can promote security features by explicitly describing privacy and security regulations and policies (Chang et al., 2016). In terms of privacy, trust can be regarded as the consumer's expectation that retailers will maintain their personal information fairly and without bias. If retailers could guarantee that the customer's private information would remain confidential without exposing it to any third party, this would allow a sustainable trust relationship between customers and retailers (Bojang, 2017). Given that most online shopping processes require personal information during online payments, security concerns become another extrinsically motivational factor that may prevent customers from making online transactions (Chang et al., 2016). Perceived security is used to illustrate the subjective probability that people will believe their sensitive information will not be seen, stored or controlled during the storage or transit process by inappropriate parties (Ong & Lin, 2015). Previous research also asserts that perceived security is positively associated with trust in e-commerce contexts (e.g., Bojang, 2017; Mukherjee & Nath, 2007). A belief that online payment methods could possibly be intercepted and are not always secure would reduce online customer trust, discouraging consumers from sharing personal information and engaging in online purchases (Mukherjee & Nath, 2007).

Moreover, third parties have emerged as essential in motivating customers to participate in online transactions (Pavlou et al., 2003; Salo & Karjaluoto, 2007). In the online context, it is likely that customers consider the support implied by external assurance suppliers as distinct from the actual assurances offered by the retailers, before they become involved in online shopping activities (Wakefield & Whitten, 2006). Studies suggest retailers should show third-party assurances in order to enhance customer trust in trading websites and to decrease perceptions of risk in online transactions (Bianchi & Andrews, 2012). Showing renowned third-party brands on the websites is a common way to boost customers' confidence in providing their information to another party, and motivating customers to engage in online purchases (Salo & Karjaluoto, 2007). It allows retailers to assure customers that their websites are indeed sufficiently credible and reliable through which to conduct online transactions (Bojang, 2017). The brands could be certifications such as ISO 9001. In a similar way the GDPR may enhance online customer trust through its emphasis on stronger rights over personal data. This leads to the three following hypotheses:

*H3. Perceived privacy is positively associated with online customer trust.*

*H4. Perceived security is positively associated with online customer trust.*

*H5. Perceived third-party assurance is positively associated with online customer trust.*

Grounded in an extension of SDT, perceived trustworthiness is also considered as an extrinsic motivation influencing customer trust. In an e-commerce context, perceived trustworthiness is the expectation that the website is trustworthy, which has been recognized as a critical factor in motivating customers' online transactions with a significant impact on a sustained trust intention (Liao et al., 2009). When customers perceive an Internet business as being trustworthy, they may extend their trust in it (Zhu & Chen, 2012). The degree to which a website can improve its openness of information will affect its ability to address online customers' demands (Mukherjee & Nath, 2003). Moreover, openness is identified as website transparency, and website interactivity in an online environment (Kim et al., 2014; La Porte et al., 2002). It may be understood as an interpretation of transparency that has high correlation with an improvement of the GDPR. This generates another hypothesis:

*H6. Perceived openness is positively associated with online customer trust.*

According to the theory of reasoned action, a customer's intention to purchase is preceded by the customer's attitude towards the purchase (Jarvenpaa et al., 2000). Online customer trust has long been recognized as playing a critical role in affecting customers' online buying behavior (Hsu et al., 2014; Pavlou & Fygenson, 2006). In particular, it has been a predominant influence on customers' online purchase intention. Meanwhile, the GDPR affirms the importance of establishing trust that allows the development of the digital economy over the European market (EUR-Lex, 2019). It is expected to provide opportunities for organizations to improve online customer trust through risk-related personal data governance (European Commission, 2019c; Wachter, 2018). The improvements (e.g., clear language, stronger rights and more information transparency) probably demonstrate that the GDPR can be highly pertinent to some antecedents of online customer trust, which affect online purchase intention in turn. This leads to the following hypothesis:

*H7. Online customer trust is positively associated with online purchase intention.*

## Research Methodology

This positivist study used a survey strategy with a deductive approach to investigate the research questions. A questionnaire was designed for primary data collection as the basis for quantitative data analysis, and to obtain results that would test the proposed hypotheses while generating new insights about the GDPR that may affect online customer trust. The study received approval from the institute's Research Ethics Committee, giving assurance that ethical considerations such as the risk of harm, and voluntary consent had been appropriately handled in the research design.

### Data collection

Any online customer whether residing in EU or non-EU countries can potentially benefit from GDPR compliance, given that the data will be processed in a more lawful manner, and the data processing and technologies will meet higher standards in the GDPR context. Thus, we considered the research population to be broad, with potential participants in our study being anyone who has online buying experience. We considered convenience sampling appropriate for data collection from students in a higher education institute in Auckland, New Zealand. A questionnaire was administered to volunteer participants through the SurveyMonkey® platform, a website-based platform allowing users to collect and store data in a single framework. To fully echo the research background as well as the GDPR's present and potential impact on global technology development, the terminology of 'the website' was introduced to the research participants as any website that they are familiar with, and where they have purchased items/services or conducted business activities already. As such, the participants responded based on their shopping experience from any commercial website they often visited.

### Measurement development

The questionnaire has three sections covering demographic, hypothesis-related, and GDPR-specific questions, as shown in Appendix C. The hypothesis-related measurement items were developed from sources discussed and tested in previous studies, including Bojang (2017), Chang and Fang (2013), Chen and Barnes (2007), Liu et al. (2017), as well as Mukherjee and Nath (2007) and use a five-point Likert scale ranging from '1' strongly disagree to '5' strongly agree. The GDPR-specific questions in the last questionnaire section include those relating to three attributes of the GDPR: the GDPR's legal authority in principle, penalty, and consent-related efficacy (see Appendix C).

A pretest of the questionnaire was run to fine tune the survey in order to improve the logical validity of the questions, the reliability and comprehensibility of statements (Hassandoust et al., 2011). Five experts with a similar background to the prospective participants were approached for their comments on the face validity of the measurement items and the clarity of the questions. Several refinements were then made to improve the flow and structure of the questions.

## Data Analysis

This study focuses on predicting the psychological factors that may have a bearing on customers' trust in websites and their online purchase intention. It utilizes the latent variable (LV) scores to estimate potential relationships among eight LVs in our structural model. Partial least square to structural equation modeling (PLS-SEM) is a causal-predictive approach to SEM that stresses prediction in assessing statistical models, where structures are developed to provide causal explanations (Hair et al., 2019). It can support not only our complex structural model that contains many constructs, indicator variables and/or relationships, but also a small population that limits the sample size (Hair et al., 2019). PLS-SEM has been extensively applied in customer-oriented studies (Tenenhaus et al., 2005). Our research utilizes PLS-SEM through SmartPLS 3.0 software to evaluate the measurement and structural model. The following section includes the demographic profile, reliability and validity analysis, assessment of the structural model, and additional findings.

### Demographic profile

We ran the survey for two weeks in March 2019 and it delivered 224 responses. After removing 24 invalid responses, our data set comprised 200 complete and valid questionnaires. Table 2 summarizes the demographic profile of the respondents. A simple analysis of these data shows that the sample is characterized by respondents who were more likely to be female (63.5%) aged under 45 years (93%), and highly educated (79% above college degree).

Table 2 - Demographic Profile of Respondents			
Measure	Items	Frequency	Percentage (%)
Gender	Female	127	63.5%
	Male	69	34.5%
	Other	1	0.5%
	Prefer not to say	3	1.5%
Age	18-24	55	27.5%
	25-34	88	44.0%
	35-44	43	21.5%
	45-54	11	5.5%
	55-64	2	1.0%
	>64	1	0.5%
Education	Less than a high school diploma	5	2.5%
	High school degree or equivalent	14	7.0%
	College, no degree	23	11.5%
	Bachelor's degree (e.g. BA, BS)	111	55.5%
	Master's degree (e.g. MA, MS)	31	15.5%
	Doctorate degree (e.g. PhD)	4	2.0%
	Other	6	3.0%
	Prefer not to say	6	3.0%



**Table 2 - Demographic Profile of Respondents**

Online buying frequency	>2 times each week	6	3.0%
	1-2 times each week	56	28.0%
	1-2 times each month	69	34.5%
	1-2 times each three months	31	15.5%
	1-2 times each half a year	32	16.0%
	Prefer not to say	6	3.0%

### Reliability and validity analysis

Using PLS-SEM, this study assessed the reliability and validity of the measurement model through several evaluation criteria including internal consistency reliability, indicator reliability, convergent validity and discriminant validity of the instrument items (Chin, 2010). In summary, indicator reliability (loadings > 0.7), internal consistency reliability (CR > 0.7,  $\alpha$  > 0.7) and convergent validity (AVE > 0.5) were evaluated and confirmed to be satisfactory as shown in Table 3.

**Table 3 - Convergent Validity Testing**

Construct	Std. loading of each item	Cronbach's Alpha ( $\alpha$ )	Composite Reliability (CR)	Average Variance Extracted (AVE)
Perceived usefulness (PU)	0.821, 0.795, 0.827, 0.753	0.813	0.876	0.639
Perceived ease-of-use (PE)	0.866, 0.89, 0.84	0.832	0.90	0.749
Perceived privacy (PP)	0.828, 0.887, 0.868, 0.82, 0.843	0.904	0.928	0.722
Perceived security (PS)	0.78, 0.832, 0.709, 0.801	0.787	0.862	0.611
Perceived third-party assurance (PTA)	0.897, 0.914, 0.866	0.872	0.921	0.796
Perceived openness (PO)	0.911, 0.851	0.717	0.875	0.777
Online customer trust (OCT)	0.856, 0.83, 0.848, 0.785	0.849	0.899	0.689
Online purchase intention (OPI)	0.936, 0.95, 0.933	0.934	0.958	0.883

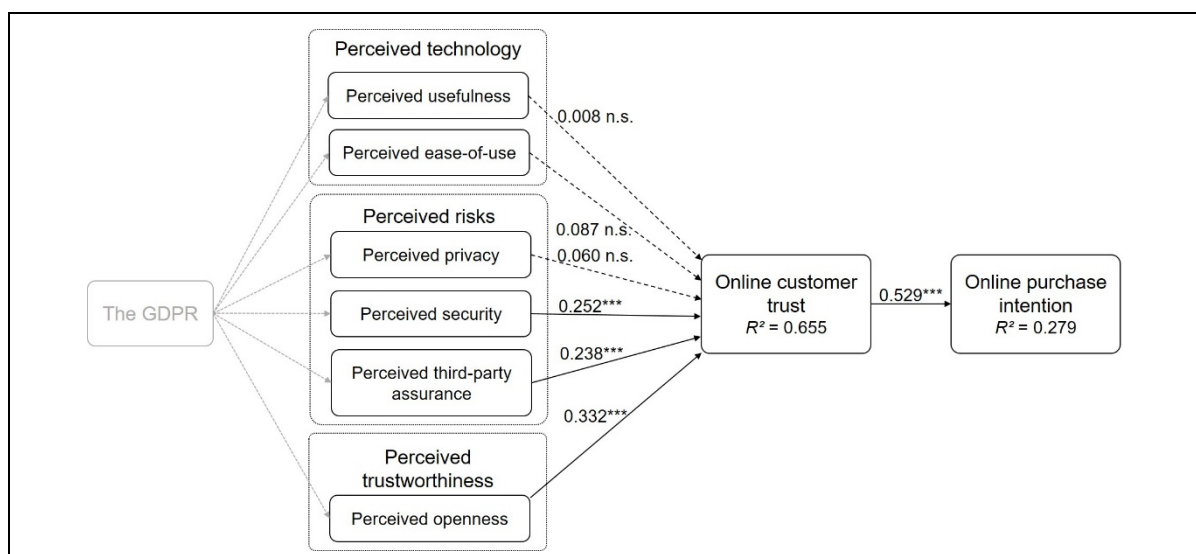
Discriminant validity was examined through Fornell and Larcker's (1981) technique. The findings from an extraction of AVE value were found to meet Fornell and Larcker's criterion, as shown in Table 4.

**Table 4 - Discriminant Validity**

	Perceived usefulness (PU)	Perceived ease-of-use (PE)	Perceived privacy (PP)	Perceived security (PS)	Perceived third-party assurance (PTA)	Perceived openness (PO)	Online customer trust (OCT)	Online purchase intention (OPI)
Perceived usefulness (PU)	<b>0.799</b>							
Perceived ease-of-use (PE)	0.708	<b>0.866</b>						
Perceived privacy (PP)	0.459	0.467	<b>0.85</b>					
Perceived security (PS)	0.576	0.581	0.727	<b>0.782</b>				
Perceived third-party assurance (PTA)	0.46	0.536	0.581	0.627	<b>0.892</b>			
Perceived openness (PO)	0.534	0.582	0.496	0.573	0.567	<b>0.882</b>		
Online customer trust (OCT)	0.529	0.588	0.59	0.69	0.67	0.696	<b>0.83</b>	
Online purchase intention (OPI)	0.569	0.541	0.292	0.415	0.496	0.535	0.529	<b>0.94</b>

### Assessment of the structural model

In PLS-SEM, the  $R^2$  measures and the significance and level of the path coefficients are the primary criteria to evaluate a structural model (Hair, et al., 2011). The evaluation results including the coefficient of determination ( $R^2$ ) are shown in Figure 2.  $R^2$  is a measure of predictive accuracy of a model (Hair et al., 2014). In marketing research area  $R^2$  values with 0.75, 0.50 or 0.25 for IVs can be considered substantial, moderate or weak, respectively; results of 0.20 are regarded as high in domains such as customer behavior (Hair et al., 2011). The results indicate that perceived privacy, security, third-party assurance and openness explain 66% of the variance in online customer trust ( $R^2=0.655$ ), and online customer trust explains 28% of the variance in online purchase intention ( $R^2=0.279$ ).

**Figure 2 - Structural Model Results**

Note: \*  $p < 0.05$ , \*\*  $p < 0.01$ , \*\*\*  $p < 0.001$ , n.s. = nonsignificant.

A bootstrapping procedure was performed to assess the statistical significance of the path coefficients. The results show that perceived usefulness, perceived ease-of-use and perceived privacy have no positively significant relationship with online customer trust as their p-values are all higher than 0.05. Thus, hypotheses H1, and H2 and H3 are disproved. The path coefficient is significant when the T-statistics are greater than 1.96 (Wong, 2013). The results indicate that perceived security is positively associated with online customer trust (path coefficient value = 0.252,  $t = 3.769$ ,  $p = 0.000$ ); perceived third-party assurance is positively associated with online customer trust (path coefficient value = 0.238,  $t = 3.801$ ,  $p = 0.000$ ); and perceived openness is positively associated with online customer trust (path coefficient value = 0.332,  $t = 5.034$ ,  $p = 0.000$ ). Notably, those significant t-values are from 3.769 to 5.034. Thus, hypotheses H4, H5 and H6 are supported. The findings also show that online customer trust has a positive significant impact on online purchase intention (path coefficient value = 0.529,  $t = 8.556$ ,  $p = 0.000$ ), validating hypothesis H7.

### Data analysis for the GDPR-specific questions

In order to identify the GDPR-specific factors that may affect online customer trust while enabling new insights about the GDPR (echoing the second research question), the attitudinal data from six GDPR-specific questions were analyzed using a quantitative approach. We coded the questions as Q1-Principle, Q2-Principle, Q1-Fine, Q2-Fine, Q1-Consent and Q2-Consent (see Appendix C). We divided them into three pairs focused on three attributes of the GDPR: legal authority in principle, penalty and consent efficacy. Q1-Principle focused on a primary impression of the GDPR as a legal authority. Q1-Fine is concerned with participants' trust when they know the retailer will be faced with high fines for disobeying a data protection law. Q1-Consent relates to participants' trust if they are asked for their consent before their data can be used by the retailer. Q1-Principle, Q1-Fine and Q1-Consent were followed by an open-ended question, namely Q2-Principle, Q2-Fine and Q2-Consent, asking participants who answered yes for Q1s to explain why. Table 5 presents a quantitative analysis summary for the results of Q1-Principle, Q1-Fine and Q1-Consent.

**Table 5 - Summary of Descriptive Statistics for Q1-Principle, Q1-Fine and Q1-Consent – GDPR Context**

Measures	Items	Frequency	Percentage (%)
If one of your favorite e-commerce websites implements the principles of the GDPR, would that increase your confidence and trust of using that website? (Q1-Principle)	Yes	67	33.5%
	No	17	8.5%
	Do not know	102	51.0%
	Prefer not to say	14	7.0%
If you know the website is going to be faced with high fines and penalties for disobeying a data protection law, would that increase your confidence and trust of using that website? (Q1-Fine)	Yes	58	29.0%
	No	74	37.0%
	Do not know	54	27.0%
	Prefer not to say	14	7.0%
If you are asked for your consent before your data can be used by the website, would that increase your confidence and trust of using that website? (Q1-Consent)	Yes	47	23.5%
	No	67	33.5%
	Do not know	68	34.0%
	Prefer not to say	18	9.0%

As part of the research design, responses from the open-ended questions (coded as Q2-Principle, Q2-Fine and Q2-Consent) were analyzed quantitatively. The most common words used by the participants about the GDPR and online trust were distilled and counted as frequencies across the data. Table 6 summarizes the frequency with which the top-ranked keywords occurred in the open-ended responses. As can be seen, seven keywords – ‘safety’, ‘protection’, ‘trust’, ‘security’, ‘law’, ‘respect’, and ‘privacy’ occurred frequently in the responses to the three open-ended questions.

**Table 6 - Occurrences of Keywords in the Responses to the Open-ended Questions**

Code	Keyword	Occurrences
Q2-Principle	Safety (or safe)	15
	Security (or secure)	9
	Protection (or protect)	7
	Trust, (or reliable, trustworthy, confident)	7
	Privacy (or private)	4
	Standard (or law)	3
Q2-Fine	Safety (or safe)	7
	Law (or rule, enforcement, supervision)	6
	Protection	5
	Trust (or reliable, believe)	4
	Security (or secure)	2
Q2-Consent	Respect	7
	Protection (or protect)	3
	Trust (or confident)	3
	Privacy	3
	Right (or authorisation)	2

## Discussion

This section explores implications of the study's findings as shown in the previous section in terms of the two research questions.

### *What are the impacts of the perceived technology, perceived risks and perceived trustworthiness on online customer trust in the GDPR context?*

Despite a study of the role of TAM in the development of trust in online shopping behavior (Koufaris & Hampton-Sosa, 2004), the findings in the present research showed that neither a potential change in perceived usefulness nor perceived ease-of-use on a website will have a significant influence on online customer trust. Both results above have been found by other studies such as those of Chen and Barnes (2007), Ejdy (2018), and Giovannini et al. (2015). Online consumption has grown dramatically since the early days of e-commerce. The majority of our study's participants were experienced customers who had bought online more than once in the previous three months. This implies their familiarity with the benefits and functions of websites – they were more likely to 'click and pay' without much thought on websites that were easy to use. Gefen (2003) argues that repeated prior behavior frequently dictates present behavior, separately from any rational assessments such as those proposed by the theory of reasoned action on which TAM is based. Habitual use of an IT application can simply appeal to consumers beyond perceived usefulness and ease-of-use. Although research has discussed the applicability of TAM to a broad variety of IT for both novice and experienced users (Gefen, 2003; Karahanna et al., 1999), TAM was originally targeted at achieving new IT adoption (Davis et al., 1992; Gefen & Straub, 2000), rather than examining its continued use (Gefen, 2003). Yet, clear language is one of the potential improvements offered by the GDPR and it is related to perceived usefulness and ease-of-use of systems. Since both perceived usefulness and ease-of-use were not positively associated with online customer trust in this study, clearer language and clearer information on websites may remain essential characteristics. However, they do not add competitive value by significantly affecting online customers' trust during repeat purchases.



Our findings indicate that perceived privacy had no significant positive effect on online customer trust among those in our sample. Experienced customers are familiar with the technologies of security and are capable of identifying the characteristics of security technologies which totally guarantee individual privacy (Roca et al., 2009). Thus, privacy concerns would probably have less importance for these customers and may not affect online customer trust significantly as a result. Another possibility could be customers' lack of awareness about privacy issues. Privacy is deemed a nebulous concept compared to security and third-party assurance, and the notion of personal data and its control may mean different things to different people (Belanger et al., 2002). According to SDT, motivations lead human behaviors, and negative extrinsic motivations such as anxiety or concerns towards external events affect intentional activities (Chang et al., 2016). Thus, it could be inferred that consumers with lower awareness of privacy concerns in online transactions are less likely to be motivated towards behaviors concerning trust.

On the other hand, our findings reveal that perceived security had a significant influence on online customer trust in our study, which is consistent with the findings of previous research (e.g., Bojang, 2017; Chen & Barnes, 2007; Koufaris & Hampton-Sosa, 2004; Mukherjee & Nath, 2007). Based on SDT, customers' perceptions regarding strong security of a trading website is considered as external motivation, implying greater protection for users and leading to positive outcomes. Increased safety of computers and financial information can increase online customer trust. The most important step for establishing online customer trust is to offer customers the guarantee that their personal information will be safeguarded (Chen & Barnes, 2007). Online retailers adopt various security enforcement principles such as protection, verification, encryption and authentication, to address online customer concerns regarding security (Chellappa & Pavlou, 2002). Perceptions of security enforcement principles positively facilitate perceived trust in online transactions (Chellappa & Pavlou, 2002). The GDPR is a suite of new rules with enhanced enforcement powers, requiring businesses to update their processes, particularly in the area of online security (Boban, 2018a). According to SDT, the GDPR can also be seen as an extrinsic motivation in relation to perceived security with an offer of personal data protection through a series of security laws and regulations, potentially stimulating online purchase trust. Thus, the GDPR would likely have a positive influence on online customer trust.

Based on our findings, perceived third-party assurance also has a significant influence on online customer trust. The finding implies that third-party assurance can be utilized to reduce customer concerns and promote trust. This result is in line with the findings of previous studies (e.g., Bianchi & Andrews, 2012; Bojang, 2017; Palmer et al., 2000; Sahney et al., 2013). However, risks remain when companies share customers' data with third-party entities (Tesfay et al., 2018). To address this issue, the GDPR requires businesses to inform customers if their personal information will be shared with third parties (EUR-Lex, 2019; Tesfay et al., 2018). In this regard, the GDPR could be seen as a dominant third-party partner, helping moderate the relationship between retailers and their third-party partners, in order to improve customer trust in the virtual world. Third-party certifications behave as risk relievers (Andrews & Boyle, 2008) in online transactions. Retailers can enhance online trust by displaying third-party certifications (Sahney et al., 2013) such as the GDPR. Indicators of third-party certifications can be web assurance seals, trust marks, and credit card symbols (Wu et al., 2010). For example, retailers can place a specific icon or logo on their websites, disclosing that they are using encryption technology for secure payment systems (Andrews & Boyle, 2008; Bianchi & Andrews, 2012). On the other hand, to improve customers' perception towards third-party assurance, the seals need to be promoted in order to have more effect on consumers. The GDPR builds a system of certification, data safeguard seals, and marks that enable personal users to quickly recognize the data protection pertinent to a product or service (Rotenberg & Jacobs, 2013). Grounded in SDT, third-party assurance has been deemed an extrinsically motivational source that promotes customers' confidence and trust to share their personal information to another party online. As such, the GDPR in the e-commerce domain can be used as either an

independent third-party assessor or a supervisor affecting third-party vendors and services involved during the online trading process.

In this study perceived openness was found to be the most influential antecedent of online customer trust. It confirms the significance of perceived openness in improving customer trust in online shopping activities. In SDT, customers can be encouraged because of the value of activities (Ryan & Deci, 2000). Perceived openness delivers a perception of freedom in sharing information and ideas, as well as in providing an open environment where rules, regulations and policies are transparent and clearly communicated. It can be used to promote customer confidence and trust as another extrinsic motivation factor. Our result supports an early study of Mukherjee and Nath (2007), where perceived openness was included in the test as one of the components of website communication and was confirmed to have a significant influence on online customer trust. Openness in communication can be defined as transparency (Kim et al., 2014), one of the main improvements offered by the GDPR. Thus, the GDPR, in terms of its contribution to information transparency, can be regarded as a potentially significant motivating factor boosting online customer trust.

According to our findings, online customer trust has a significant positive impact on customers' purchase intention online. Customers' trust in online transactions significantly increases their intention to purchase online. Previous studies also supported a positive association between customers' trust and their online purchase intentions (e.g., Chen & Barnes, 2007; Das, 2016; Hsiao et al., 2010; Yoon, 2002). Research has shown that high levels of customer trust encourage online buying intention and help retain online customers (Gefen & Straub, 2004), while a lack of faith is the main reason that customers give up buying online (Hoffman et al., 1999). Online customer trust facilitates e-commerce (Gefen & Straub, 2004), which resonates with the GDPR's affirmation: the creation of trust is important because it allows the development of the digital economy over the internal market (EUR-Lex, 2019).

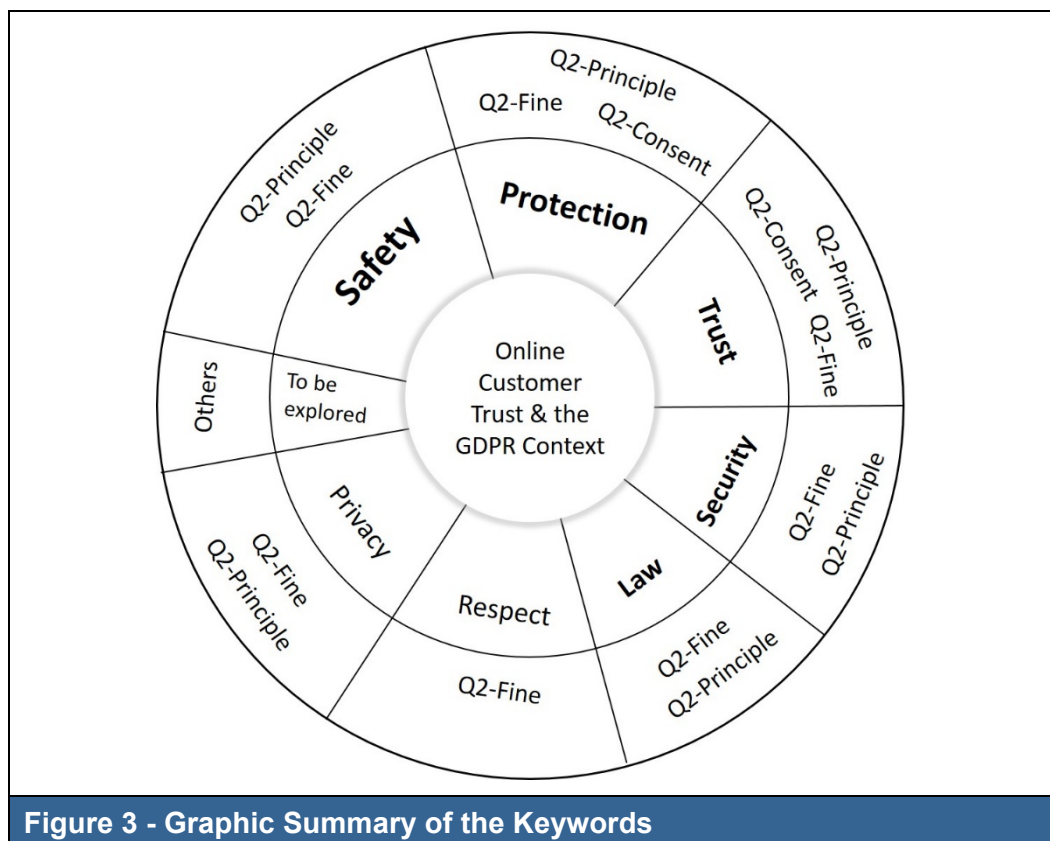
### ***What are the GDPR-specific factors that may affect online customer trust?***

Regarding Q1-Principle, our findings reveal that almost half of the participants are not familiar (or unconcerned) with the GDPR. More participants answered yes than answered no for the Q1-Principle, showing that they agreed that the implementation of the GDPR's principles would increase their confidence and trust in commercial websites. This result coincides with the argument from Cross (2005) that the law may facilitate perceived trust. By providing legal assurances of solutions or remedies for trust breaches, parties are more likely to be both trustworthy and trusting (Cross, 2005). Hence, the GDPR can be expected to be a special law-based determinant factor being used to influence online customer trust. Several keywords appeared in the responses to the Q2-Principle including 'safety', 'security', 'protection', 'trust' and 'privacy'. A typical response was, "I think my personal information and financial information are safer", which may indicate that the GDPR implementation provides stronger security in the participants' minds.

In terms of Q2-Fine, most of the participants did not believe that high fines for disobeying a data protection law would increase their trust in a website. This result may induce more curiosity about exploring the relationship between trust and restrictions from monetary penalties, the relationship between sellers and buyers under a strict penalty system, or a trust transfer among parties. The keywords – 'safety', 'law', 'protection', 'trust', and 'security' were observed to have high occurrences respectively. Examples of the explanatory comments were "feel more safe", "it will limit the law breaking", "because they will do their best to not lose money", and "my information can be well protected", among others. The order of the keywords hints that people may pay more attention to 'safety', 'law' and 'protection' while thinking about the relationship between fines and online trust. Customers may assume that retailers have to try their best to protect customer data in order to avoid high fines.

Regarding Q2-Consent, over half of the respondents who answered yes for the Q1-Consent, believed that asking about consent before their data was shared would not increase their trust. Interestingly, 'respect' was the top-ranked word used by the participants to explain their understanding of the GDPR's consent topic. For example, one of the respondents stated that "I feel respected." Other words such as 'protection', 'trust', 'privacy', and 'right' or 'authorization' also ranked highly in the answers. Consent from users is one of five improvements brought by the GDPR. However, the findings showed that consent seemed to be related to courtesy or respectful behavior, rather than to privacy and rights. One participant commented, "at least will ask your opinion", which can be understood that although s/he did not know what happened behind the scenes, at least s/he was asked when her/his data was used. Only two respondents mentioned rights or authorization. This reflects a weak awareness of the relationship between consent and personal rights on data protection.

Figure 3 graphically illustrates the participants' most commonly used words in answering the three open-ended questions. The graphic aims to suggest some similarities in the ways they looked at the GDPR in terms of online customer trust, and to seek a clearer understanding of relationships between the keywords. The text size indicates graphically the relative frequency of occurrences of these words.



**Figure 3 - Graphic Summary of the Keywords**

## Theoretical and Practical Contributions

This study offers new insights into the adaptation of SDT for online customer trust research in the context of the GDPR. Motivation theory has been shown to have a significant impact on both behavior and behavioral intention across many studies. It has been a stream of IS research that aims to explain factors affecting technology acceptance. SDT acts as the basis for enabling examination of motivation-based factors in the theoretical models of trust. In light of SDT, the present study affirms that perceived risks and trustworthiness can assist development of the research model, allowing relevant trust antecedents to be regarded as extrinsic motivations for customers' online trust, and better exploring the role of the GDPR in the Internet-based trust domain. This represents an opportunity to include law-related motivational elements into trust research, enabling more investigation of the impact of regulations and certifications on online customer trust.

Another contribution is the identification of GDPR-related constructs, in the online trust theoretical models. The GDPR has been identified as affecting online customer trust, by playing a role related to perceived security, third-party assurance and perceived openness of information. The two former factors are highly linked to strong rights, one of the key improvements of the new GDPR, while the latter one is associated with 'more transparency' – another improvement of the GDPR. Through the emergence of the GDPR, factors that may have been previously neglected which are nevertheless playing a significant role in shaping customers' online trust from a legal perspective are able to be discussed in trust research. These include safety, protection, trust, security, law, respect, and privacy.

This study offers practical contributions in various ways for the management strategies of online retailers and e-commerce practitioners. Firstly, it arouses a focus on the role of the GDPR in helping businesses improve trust in the e-commerce context. The study should attract managers' attention to the GDPR, not only because it imposes stricter requirements on personal data security, but also because of its capability to improve customer trust. Organizations can use the principles of the GDPR to enhance their data protection policies and customer trust. Secondly, this research provides straightforward suggestions on the critical aspects of online trust that can significantly affect it. These antecedents have been confirmed to affect online customer trust significantly and have a strong tie to the GDPR. Businesses may pay more attention to these confirmed antecedents of trust when they are developing trust towards online customers. For example, they can enhance the transparency and openness of their websites, by clearly informing online customers about why and how they will use customers' data, and informing customers if the decision is automated and offering users the chance to dispute it.

Thirdly, this study can provide a theoretical basis for those e-commerce companies which are under GDPR compliance, for developing and deploying a plan for trust improvement. Based on the regression equation formula, it allows those companies to determine which aspects of trust antecedents are essential and worthy of more investment. For instance, considering that perceived usefulness and perceived ease-of-use do not appear to play a critical role in customers' online trust, organizations can incorporate perceived usefulness and perceived ease-of-use in a long-term trust improvement plan, and treat them as routine but not urgent tasks (low priority), with less human resource and capital investment required. In addition, this research can also provide help for those international companies which have customers from EU countries, and which need to evaluate their customer trust status in the GDPR context. As mentioned, trust can be treated as a multi-dimensional concept to address problems in the real business world. Organizations would focus on the constructs in the research model to undertake market investigations. In addition, this research may help EU authorities who are operating the GDPR by presenting them with stakeholder feedback from academic research. As a result, this kind of study may support future improvements in the GDPR.



## Limitations and Future Research

While the findings of this research have implications for both research and practice, they need to be viewed with respect to certain limitations. First, the present research adopted a cross-sectional study to collect data at a specific point in time, that could limit the cause and effect significance of the results. Future studies may find it necessary to investigate any changes in the GDPR-related factors and customers' online trust over time through a longitudinal study. Second, the survey results may have been influenced by the sample selection bias of convenience sampling which could be seen as a limitation to the generalizability of this study. Third, the scope of the GDPR involved in the present research has been explored from the perspective of perceived technology, risks and trustworthiness. This scope is expected to involve more novelty features in future research. Future research may be based on a wider literature review of the GDPR for a more in-depth study. For example, a thorough investigation of the role of the data protection officer could help resolve the issue that people must trust a man-made object (the technology) instead of a real human being. European residents should be part of the target sample group in future studies as they are more likely to be familiar with the GDPR.

## Conclusions

Trust plays an essential role in promoting successful relationships, reducing risk and uncertainty, and increasing willingness to purchase. Many studies have emphasized that online customer trust positively influences customers' online purchase intention. The GDPR is a new legal framework that has been expected to increase user trust, and the transparency and accountability of websites, as well as to influence the legal frameworks of other non-EU countries (Addis & Kutar, 2018). As few studies have explored online customer trust from the GDPR perspective, this study has focused on filling this gap by drawing on TAM and SDT, and has examined the antecedents of online customer trust from the GDPR perspective. Five improvements from the GDPR were identified and some of them (clear language, stronger rights, and more transparency) are found consistent with six antecedents of online customer trust in existing frameworks. Through hypothesis testing, several GDPR-related trust antecedents – perceived security, perceived third-party assurance, and perceived openness have been found to have positive significance in terms of online customer trust. Moreover, online customer trust has been confirmed to have a significant positive relationship with online purchase intention. The GDPR plays a significant role in online customer trust by bringing about stronger rights and more transparency for online customers. In addition, the GDPR can be seen as a special law-based determinant factor affecting online customer trust. This study has also generated insights about the GDPR that may affect online customer trust, but which to date have little presence in frameworks of the antecedents of online customer trust. Moreover, seven keywords – 'safety', 'protection', 'trust', 'security', 'law', 'respect', and 'privacy' have been drawn from the study's findings to represent a composite picture of how the participants in this research looked at the GDPR.

## References

- Addis, M. C., & Kutar, M. (2018). The General Data Protection Regulation (GDPR), emerging technologies and UK organizations: Awareness, implementation and readiness. *Proceedings of UK Academy for Information Systems Conference 2018*, 29.
- Akhlaq, A., & Ahmed, E. (2013). The effect of motivation on trust in the acceptance of Internet banking in a low income country. *The International Journal of Bank Marketing*, 31(2), 115-125.
- Altmayer, O. A. (2018). The tipping point – Reevaluating the Asnef-Equifax separation of competition of data privacy law in the wake of the 2017 Equifax data breach. *Northwestern Journal of International Law & Business*, 39(1), 37-58.
- Amin, M., Rezaei, S., & Abolghasemi, M. (2014). User satisfaction with mobile websites: The impact of perceived usefulness (PU), perceived ease of use (PEOU) and trust. *Nankai Business Review International*, 5(3), 258-274.
- Andrews, L., & Boyle, M. V. (2008). Consumers' accounts of perceived risk online and the influence of communication sources. *Qualitative Market Research: An International Journal*, 11(1), 59-75.
- Bandyopadhyay, S., & Bandyopadhyay, K. (2018). The European general data protection regulation and competitiveness of firms. *Competition Forum*, 16(1), 50-55.
- Bart, Y., Shankar, V., Sultan, F., & Urban, G. L. (2005). Are the drivers and role of online trust the same for all web sites and consumers? A large-scale exploratory empirical study. *Journal of Marketing*, 69(4), 133-152.
- Bauman, A. (2015). The use of the repertory grid technique in online trust research. *Qualitative Market Research*, 18(3), 362-382.
- Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *The Journal of Strategic Information Systems*, 11(3-4), 245-270.
- Beldad, A., De Jong, M., & Steehouder, M. (2010). How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. *Computers in Human Behavior*, 26(5), 857-869.
- Bianchi, C., & Andrews, L. (2012). Risk, trust, and consumer online purchasing behavior: A Chilean perspective. *International Marketing Review*, 29(3), 253-275.
- Boban, M. (2018a). Cyber security foundations for compliance within GDPR for business information systems. *Proceedings of the 35th International Scientific Conference on Economic and Social Development – Sustainability from an Economic and Social Perspective*, 541-553. Varazdin, Croatia.
- Boban, M. (2018b). Protection of personal data and public and private sector provisions in the implementation of the general EU directive on personal data (GDPR). *Proceedings of the 27th International Scientific Conference on Economic and Social Development*, 161-169. Varazdin, Croatia.
- Bojang, I. (2017). Determinants of trust in B2C e-commerce and their relationship with consumer online trust: A case of Ekaterinburg, Russian Federation. *Journal of Internet Banking and Commerce* 22(8), 1-59.
- Butler, Jr, J. K. (1991). Toward understanding and measuring conditions of trust: Evolution of a conditions of trust inventory. *Journal of Management*, 17(3), 643-663.

- Çelik, H. (2011). Influence of social norms, perceived playfulness and online shopping anxiety on customers' adoption of online retail shopping. *International Journal of Retail & Distribution Management*, 39(6), 390-413.
- Centre for International Governance Innovation. (2019). *2017 CIGI-Ipsos Global Survey on Internet Security and Trust*. Retrieved from [https://www.cigionline.org/sites/default/files/documents/CIGI-Ipsos%202017%20Full%20Report\\_0.pptx](https://www.cigionline.org/sites/default/files/documents/CIGI-Ipsos%202017%20Full%20Report_0.pptx)
- Chang, S. H., Chih, W. H., Liou, D. K., & Yang, Y. T. (2016). The mediation of cognitive attitude for online shopping. *Information Technology & People*, 29(3), 618-646.
- Chang, Y., & Fang, S. (2013). Antecedents and distinctions between online trust and distrust: Predicting high- and low-risk Internet behaviors. *Journal of Electronic Commerce Research*, 14(2), 149-166.
- Chellappa, R. K., & Pavlou, P. A. (2002). Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logistics Information Management*, 15(5/6), 358-368.
- Chen, S. C., & Dhillon, G. S. (2003). Interpreting dimensions of consumer trust in e-commerce. *Information Technology and Management*, 4(2-3), 303-318.
- Chen, Y. H., & Barnes, S. (2007). Initial trust and online buyer behavior. *Industrial Management & Data Systems*, 107(1), 21-36.
- Chin, W. W. (2010). How to write up and report PLS analyses. In V. Esposito Vinzi, W. W. Chin, J. Henseler, & H. Wang, *Handbook of partial least squares* (pp. 655-690). Berlin, Heidelberg: Springer.
- Chirica, S. (2017). The main novelties and implications of the new general data protection regulation. *Perspectives of Business Law Journal*, 6(1), 159-176.
- Cho, Y. C., & Sagynov, E. (2015). Exploring factors that affect usefulness, ease of use, trust, and purchase intention in the online environment. *International Journal of Management & Information Systems (Online)*, 19(1), 21-36.
- Chong, A. Y., Ooi, K., Lin, B., & Tan, B. (2010). Online banking adoption: An empirical analysis. *The International Journal of Bank Marketing*, 28(4), 267-287.
- Chow, S., & Holden, R. (1997). Toward an understanding of loyalty: The moderating role of trust. *Journal of Managerial Issues*, 9(3), 275-298.
- Ciriani, S. (2015). The economic impact of the European reform of data protection. *Communications & Strategies*, (97), 41-58.
- Clark, M., Davidson, R., Hanrahan, V., & Taylor, N. E. (2017). Public trust in policing: A global search for the genetic code to inform policy and practice in Canada. *Journal of Community Safety and Well-Being*, 2(3), 101-111.
- Corritore, C. L., Kracher, B., & Wiedenbeck, S. (2003). On-line trust: Concepts, evolving themes, a model. *International Journal of Human-Computer Studies*, 58(6), 737-758.
- Cross, F. B. (2005). *Law and trust*. (Law and Economic Working Paper No. 064). Austin: The University of Texas.
- Das, G. (2016). Antecedents and consequences of trust: An e-tail branding perspective. *International Journal of Retail & Distribution Management*, 44(7), 713-730.
- Das, T. K., & Teng, B. (2004). The risk-based view of trust: A conceptual framework. *Journal of Business and Psychology*, 19(1), 85-116.
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 3(13), 319-340.

- Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: a comparison of two theoretical models. *Management Science*, 35(8), 982-1003.
- Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1992). Extrinsic and intrinsic motivation to use computers in the workplace. *Journal of Applied Social Psychology*, 22(14), 1111-1132.
- Davis, R., Sajtos, L., & Chaudhri, A. A. (2011). Do consumers trust mobile service advertising? *Contemporary Management Research*, 7(4), 245-269.
- Deci, E. L., & Ryan, R. M. (2008). Self-determination theory: A macrotheory of human motivation, development, and health. *Canadian Psychology*, 49(3), 182-185.
- Deci, E. L., Vallerand, R. J., Pelletier, L. G., & Ryan, R. M. (1991). Motivation and education: The self-determination perspective. *Educational Psychologist*, 26(3-4), 325-346.
- De Hert, P., & Czerniawski, M. (2016). Expanding the European data protection scope beyond territory: Article 3 of the general data protection regulation in its wider context. *International Data Privacy Law*, 6(3), 230-243.
- Ejdys, J. (2018). Building technology trust in ICT application at a University. *International Journal of Emerging Markets*, 13(5), 980-997.
- EUR-Lex. (2019). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016*. Retrieved February 13, 2020, from <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1384-1-1>
- European Commission. (2019a). *A new era for data protection in the EU: What changes after May 2018*. Retrieved from [https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-changes\\_en.pdf](https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-changes_en.pdf)
- European Commission. (2019b). *CEAOB International equivalence and adequacy sub-group terms of reference and work plan 2017/2018*. Retrieved from [https://ec.europa.eu/info/sites/info/files/ceaob-subgroups-2018-equivalence-terms\\_en.pdf](https://ec.europa.eu/info/sites/info/files/ceaob-subgroups-2018-equivalence-terms_en.pdf)
- European Commission. (2019c) *The GDPR: New opportunities, new obligations*. Retrieved from [https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-sme-obligations\\_en.pdf](https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-sme-obligations_en.pdf)
- European Commission. (2019d). *What data can we process and under which conditions?* Retrieved February 13, 2020, from [https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/what-data-can-we-process-and-under-which-conditions\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/what-data-can-we-process-and-under-which-conditions_en)
- European Commission. (2019e). *What does the General Data Protection Regulation (GDPR) govern?* Retrieved February 13, 2020, from [https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_en)
- Fagan, M. H., Neill, S., & Wooldridge, B. R. (2008). Exploring the intention to use computers: An empirical investigation of the role of intrinsic motivation, extrinsic motivation, and perceived ease of use. *The Journal of Computer Information Systems*, 48(3), 31-37.
- Fishbein, M. & Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research*. Reading, MA: Addison-Wesley Publishing Company.
- Forbes.com. (2019a). *Facebook privacy update: Mark Zuckerberg's response to Cambridge Analytica scandal one year on*. Retrieved February 13, 2020, from <https://www.forbes.com/sites/daveywinder/2019/03/17/facebook-privacy-update-mark-zuckerbergs-response-to-cambridge-analytica-scandal-one-year-on/#707260612198>
- Forbes.com. (2019b). *Mark Zuckerberg addresses 'breach of trust' In Facebook user data crisis*. Retrieved February 13, 2020, from



<https://www.forbes.com/sites/kathleenchaykowski/2018/03/21/mark-zuckerberg-addresses-breach-of-trust-in-facebook-user-data-crisis/#2f32c61b3e36>

- Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 18(1), 39-50.
- French, A. M. (2017). Let's meet offline. *Information Technology & People*, 30(4), 946-968.
- Gefen, D. (2003). TAM or just plain habit: A look at experienced online shoppers. *Journal of Organizational and End User Computing*, 15(3), 1-13.
- Gefen, D., Karahanna, E., & Straub, D. W. (2003a). Trust and TAM in online shopping: An integrated model. *MIS Quarterly*, 27(1), 51-90.
- Gefen, D., Rao, V. S., & Tractinsky, N. (2003b). The conceptualization of trust, risk and their relationship in electronic commerce: The need for clarifications. *Proceedings of the 36th Hawaii International Conference on System Sciences*.
- Gefen, D., & Straub, D. W. (2004). Consumer trust in B2C e-commerce and the importance of social presence: Experiments in e-Products and e-Services. *Omega*, 32(6), 407-424.
- Gefen, D., & Straub, D. W. (2000). The relative importance of perceived ease of use in IS adoption: A study of e-commerce adoption. *Journal of the Association for Information Systems*, 1(1), 8.
- Giovannini, C. J., Ferreira, J. B., da Silva, J. F., & Ferreira, D. B. (2015). The effects of trust transference, mobile attributes and enjoyment on mobile trust. *Brazilian Administration Review*, 12(1), 88-108.
- Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research*, 59(6), 703-705.
- Goodman, B., & Flaxman, S. (2017). European Union regulations on algorithmic decision making and a "right to explanation". *AI Magazine*, 38(3), 50-57.
- Grabner-Kräuter, S., & Kaluscha, E. A. (2003). Empirical research in on-line trust: a review and critical assessment. *International Journal of Human-Computer Studies*, 58(6), 783-812.
- Greenberg, R., Wong-On-Wing, B., & Lui, G. (2008). Culture and consumer trust in online businesses. *Journal of Global Information Management*, 16(3), 26-44.
- Gurung, A., & Raja, M. K. (2016). Online privacy and security concerns of consumers. *Information and Computer Security*, 24(4), 348-371.
- Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice*, 19(2), 139-152.
- Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, 31(1), 2-24.
- Hair, J.F., Sarstedt, M., Hopkins, L., & Kuppelwieser, V.G. (2014). Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research. *European Business Review*, 26(2), 106-121.
- Hassandoust, F., Logeswaran, R., & Farzaneh Kazerouni, M. (2011). Behavioral factors influencing virtual knowledge sharing: Theory of reasoned action. *Journal of Applied Research in Higher Education*, 3(2), 116-134.
- Hassanein, K., & Head, M. (2007). Manipulating perceived social presence through the web interface and its impact on attitude towards online shopping. *International Journal of Human-Computer Studies*, 65(8), 689-708.

- Hoffman, D. L., Novak, T. P., & Peralta, M. (1999). Building consumer trust online. *Communications of the ACM*, 42(4), 80-85.
- Hsiao, K. L., Lin, J. C., Wang, X. Y., Lu, H. P., & Yu, H. (2010). Antecedents and consequences of trust in online product recommendations: An empirical study in social shopping. *Online Information Review*, 34(6), 935-953.
- Hsu, M. H., Chuang, L. W., & Hsu, C. S. (2014). Understanding online shopping intention: The roles of four types of trust and their antecedents. *Internet Research*, 24(3), 332-352.
- Hunter, L. M., Kasouf, C. J., Celuch, K. G., & Curry, K. A. (2004). A classification of business-to-business buying decisions: Risk importance and probability as a framework for e-business benefits. *Industrial Marketing Management*, 33(2), 145-154.
- Jarvenpaa, S. L., Tractinsky, N., & Vitale, M. (2000). Consumer trust in an Internet store. *Information Technology and Management*, 1(1-2), 45-71.
- Karahanna, E., Straub, D. W., & Chervany, N. L. (1999). Information technology adoption across time: A Cross sectional comparison of pre-adoption and post-adoption beliefs. *MIS Quarterly*, 23(2), 183-213.
- Kaziliunas, A. (2010). Success factors for quality management systems: Certification benefits. *Intellectual Economics*, 2(8), 30-38.
- Kim, B., Hong, S., & Cameron, G. T. (2014). What corporations say matters more than what they say they do? A test of a truth claim and transparency in press releases on corporate websites and Facebook pages. *Journalism and Mass Communication Quarterly*, 91(4), 811-829.
- Kim, D. J., Yim, M., Sugumaran, V., & Rao, H. R. (2016). Web assurance seal services, trust and consumers' concerns: An investigation of e-commerce transaction intentions across two nations. *European Journal of Information Systems*, 25(3), 252-273.
- Kim, J. B. (2012). An empirical study on consumer first purchase intention in online shopping: integrating initial trust and TAM. *Electronic Commerce Research*, 12(2), 125-150.
- Kim, J., Jin, B., & Swinney, J. L. (2009). The role ofetail quality, e-satisfaction and e-trust in online loyalty development process. *Journal of Retailing and Consumer Services*, 16(4), 239-247.
- Kimery, K. M., & McCord, M. (2002). Third-party assurances: Mapping the road to trust in e-retailing. *Journal of Information Technology Theory and Application*, 4(2), 63-82.
- Koehn, D. (2003). The nature of and conditions for online trust. *Journal of Business Ethics*, 43(1/2), 3-19.
- Köksal, Y., & Penez, S. (2015). An investigation of the important factors influence web trust in online shopping. *Journal of Marketing and Management*, 6(1), 28-40.
- Koufaris, M., & Hampton-Sosa, W. (2004). The development of initial trust in an online company by new customers. *Information & Management*, 41(3), 377-397.
- Kuhn, M. L. (2018). 147 million social security numbers for sale: Developing data protection legislation after mass cybersecurity breaches. *Iowa Law Review*, 104(1), 417-445.
- Kumar, R. R., Israel, D., & Malik, G. (2018). Explaining customer's continuance intention to use mobile banking apps with an integrative perspective of ECT and Self-determination theory. *Pacific Asia Journal of the Association for Information Systems*, 10(2), 79-112.
- La Porte, T., M., Demchak, C. C., & De Jong, M. (2002). Democracy and bureaucracy in the age of the web: Empirical findings and theoretical speculations. *Administration & Society*, 34(4), 411-446.

- Lee, M. K., & Turban, E. (2001). A trust model for consumer Internet shopping. *International Journal of Electronic Commerce*, 6(1), 75-91.
- Lewicki, R. J., & Bunker, B. B. (1995). Trust in relationships: A model of development and decline. *Conflict, Cooperation, and, Justice*, Jossey-Bass, San Francisco, CA, 133-173.
- Li, H., Yu, L., & He, W. (2019). The impact of GDPR on global technology development. *Journal of Global Information Technology Management*, 22(1), 1-6.
- Liao, Q., Luo, X., & Gurung, A. (2009). Rebuilding post-violation trust in B2C electronic commerce. *Journal of Organizational and End User Computing*, 21(1), 60-74.
- Liu, F., Xiao, B., Lim, E. T. K., & Chee-Wee, T. (2017). The art of appeal in electronic commerce. *Internet Research*, 27(4), 752-771.
- Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, 20(3), 709-734.
- McKnight, D. H., & Chervany, N. L. (2001). What trust means in e-commerce customer relationships: An interdisciplinary conceptual typology. *International Journal of Electronic Commerce*, 6(2), 35-59.
- Menon, M. (2019). GDPR and data powered marketing: The beginning of a new paradigm. *Journal of Marketing Development and Competitiveness*, 13(2), 73-84.
- Monswé, T.P., Dellaert, B.G.C., & De Ruyter, K. (2004) What drives consumers to shop online? A literature review. *International Journal of Service Industry Management*, 15(1), 102-121.
- Moon, J. W., & Kim, Y. G. (2001). Extending the TAM for a World-Wide-Web context. *Information & management*, 38(4), 217-230.
- Mou, J., & Cohen, J. (2015). Antecedents of trust in electronic-service providers: results from a meta-analysis. *Pacific Asia Journal of the Association for Information Systems*, 7(1), 1-30.
- Mukherjee, A., & Nath, P. (2003). A model of trust in online relationship banking. *The International Journal of Bank Marketing*, 21(1), 5-15.
- Mukherjee, A., & Nath, P. (2007). Role of electronic trust in online retailing. *European Journal of Marketing*, 41(9), 1173-1202.
- Oliveira, T., Alinho, M., Rita, P., & Dhillon, G. (2017). Modelling and testing consumer trust dimensions in e-commerce. *Computers in Human Behavior*, 71, 153-164.
- Ong, C., & Lin, Y. (2015). Security, risk, and trust in individuals' internet banking adoption: An integrated model. *International Journal of Electronic Commerce Studies*, 6(2), 343-355.
- Palmer, J. W., Bailey, J. P., & Faraj, S. (2000). The role of intermediaries in the development of trust on the WWW: The use and prominence of trusted third parties and privacy statements. *Journal of Computer-Mediated Communication*, 5(3).
- Parris, D. L., Dapko, J. L., Arnold, R. W., & Arnold, D. (2016). Exploring transparency: A new framework for responsible business management. *Management Decision*, 54(1), 222-247.
- Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce*, 7(3), 101-134.
- Pavlou, P. A., & Fygenson, M. (2006). Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior. *MIS Quarterly*, 30(1), 115-143.
- Pavlou, P. A., Tan, Y. H., & Gefen, D. (2003). The transitional role of institutional trust in online interorganizational relationships. *Proceedings of the 36th Annual Hawaii International Conference on System Sciences*.

- Pikkarainen, T., Pikkarainen, K., Karjaluoto, H., & Pahnla, S. (2004). Consumer acceptance of online banking: an extension of the technology acceptance model. *Internet Research*, 14(3), 224-235.
- Reimers, V., Chao, C. W., & Gorman, S. (2016). Permission email marketing and its influence on online shopping. *Asia Pacific Journal of Marketing and Logistics*, 28(2), 308-322.
- Ribbink, D., Van Riel, A. C., Liljander, V., & Streukens, S. (2004). Comfort your online customer: quality, trust and loyalty on the internet. *Managing Service Quality*, 14(6), 446-456.
- Roca, J. C., García, J. J., & De la Vega, J. J. (2009). The importance of perceived trust, security and privacy in online trading systems. *Information Management & Computer Security*, 17(2), 96-113.
- Rotenberg, M., & Jacobs, D. (2013). Updating the law of information privacy: The new framework of the European Union. *Harvard Journal of Law and Public Policy*, 36(2), 605-652.
- Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *The Academy of Management Review*, 23(3), 393-404.
- Ryan, R. M., & Deci, E. L. (2000). Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *American Psychologist*, 55(1), 68-78.
- Sahney, S., Ghosh, K., & Shrivastava, A. (2013). Conceptualizing consumer "trust" in online buying behavior: An empirical inquiry and model development in Indian context. *Journal of Asia Business Studies*, 7(3), 278-298.
- Salo, J., & Karjaluoto, H. (2007). A conceptual model of trust in the online environment. *Online Information Review*, 31(5), 604-621.
- Singh, M., & Matsui, Y. (2017). How long tail and trust affect online shopping behavior: An extension to UTAUT2 framework. *Pacific Asia Journal of the Association for Information Systems*, 9(4), 1-23.
- Tenenhaus, M., Vinzi, V. E., Chatelin, Y. M., & Lauro, C. (2005). PLS path modeling. *Computational Statistics & Data Analysis*, 48(1), 159-205.
- Tesfay, W. B., Hofmann, P., Nakamura, T., Kiyomoto, S., & Serna, J. (2018). PrivacyGuide: Towards an implementation of the EU GDPR on Internet privacy policy evaluation. *Proceedings of the Fourth ACM International Workshop on Security and Privacy Analytics*, 15-21.
- Vallerand, R. J. (1997). Toward a hierarchical model of intrinsic and extrinsic motivation. *Advances in Experimental Social Psychology*, 29, 271-360.
- Van der Heijden, H., Verhagen, T., & Creemers, M. (2003). Understanding online purchase intentions: Contributions from technology and trust perspectives. *European Journal of Information Systems*, 12(1), 41-48.
- Van Esterik-Plasmeijer, P. W. J., & Van Raaij, W. F. (2017). Banking system trust, bank trust, and bank loyalty. *The International Journal of Bank Marketing*, 35(1), 97-111.
- Voss, W. G. (2017). European Union data privacy law reform: General Data Protection Regulation, privacy shield, and the right to delisting. *Business Lawyer*, 72(1), 221-233.
- Wachter, S. (2018). Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR. *Computer Law & Security Review*, 34(3), 436-449.
- Wakefield, R. L., & Whitten, D. (2006). Examining user perceptions of third-party organizations credibility and trust in an e-retailer. *Journal of Organizational and End User Computing*, 18(2), 1-19.

- Wang, Y. D., & Emurian, H. H. (2005). An overview of online trust: Concepts, elements, and implications. *Computers in Human Behavior*, 21(1), 105-125.
- Wolters, P. T. J. (2018). The control by and rights of the data subject under the GDPR. *Journal of Internet Law*, 22(1), 6-18.
- Wong, K. K. K. (2013). Partial least squares structural equation modeling (PLS-SEM) techniques using SmartPLS. *Marketing Bulletin*, 24(1), 1-32.
- Wu, G., Hu, X., & Wu, Y. (2010). Effects of perceived interactivity, perceived web assurance and disposition to trust on initial online trust. *Journal of Computer-Mediated Communication*, 16(1), 1-26.
- Wu, J., & Lu, X. (2013). Effects of extrinsic and intrinsic motivators on using utilitarian, hedonic, and dual-purposed information systems: A meta-analysis. *Journal of the Association for Information Systems*, 14(3), 153-191.
- Xiao, L., Guo, Z., D'Ambra, J., & Fu, B. (2016). Building loyalty in e-commerce. *Program*, 50(4), 431-461.
- Yoon, S. J. (2002). The antecedents and consequences of trust in online-purchase decisions. *Journal of Interactive Marketing*, 16(2), 47-63.
- Yu, P. L., Balaji, M. S., & Kok, W. K. (2015). Building trust in internet banking: a trustworthiness perspective. *Industrial Management & Data Systems*, 115(2), 235-252.
- Zhu, Y. Q., & Chen, H. G. (2012). Service fairness and customer satisfaction in internet banking: Exploring the mediating effects of trust and customer value. *Internet Research*, 22(4), 482-498.
- Zunko, I. M. (2017). EU personal data protection rules for digital age. *Proceedings of the 22nd International Scientific Conference on Economic and Social Development*, 57-66.



## Appendix A

### Five improvements brought by the GDPR

Improvement	Explanation	Legal articles and academic sources
Clear language	Privacy policies of organizations are to be written in a straightforward and clear language.	According to Article 12 (1), this information should be provided in a concise, intelligible, transparent and effortlessly accessible form, using plain and clear language (Goodman & Flaxman, 2017; Wolters, 2018).
Stronger rights	Users have to be informed by organizations without delay in the event of harmful personal data breach, (e.g., if the data are stolen). Users can move their data to another competing service (e.g., to another platform of social media). Users have the right to access and have a copy of their data that organizations keep; users hold a clearly defined “right to erasure” or “right to be forgotten” with well-defined safeguards.	According to Article 33 (1), the data controller is obligated to inform the supervisory authority of the personal data breach “not later than 72 hours after having been aware of it” (Voss, 2017, p. 229), unless the personal data breach is unlikely to cause a risk to the freedoms and rights of natural persons (Voss, 2017). Article 15 indicates that data subjects have the right to acquire, from the data controller, confirmation of whether their personal data is being processed. This article also grants the right of data subjects to get a copy of the processed data (Wolters, 2018). With the title of Right to rasure (Voss, 2017), Article 17 is a principle being regarded as the most essential step forwards for the new framework, which allows users to request the deletion or removal of personal data if no convincing reason exists any more for the processing (Boban, 2018b).
More transparency	Organizations have to clearly inform users when transferring their data outside the EU. Organizations have to collect and process personal data only for a clear purpose, and they must inform users about new purposes if they are different from the purpose initially announced for data processing. Organizations have to inform users if the decision is automated, and offer them the opportunity to dispute it.	The GDPR has many provisions that improve trust and transparency (Wachter, 2018). Organizations often process and collect person data for different purposes other than the original reason without notifying their users about it. Article 5 (1) highlights the purpose limitation where data has to be collected for specified, legitimate and explicit purposes and is not allowed to be further processed in a way that is inconsistent with its initial purposes. According to Articles 13(2), data subjects have the right to meaningful information regarding the existence of automated decision-making, the logic engaged, and the significance and envisaged results of such processing towards data subjects (Wolters, 2018). In turn, Article 22(1) regulates that data subjects have the right not to be subject to a decision based uniquely on automated processing containing profiling, which generates legal effects towards the data subjects or significantly influences them (Wolters, 2018). In Preamble 39 of the GDPR (EUR-Lex, 2019), the principle of transparency requires that any communication and information relevant to the processing of users’ personal data be easy to understand and easily accessible and that plain and unambiguous language be used. Transparency is a determinant of OCT (Van Esterik-Plasmeijer & Van Raaij, 2017) that has been discussed in the section on the antecedents of OCT.

Consent from the user	An affirmative consent needs to be given by users before their data can be used by organizations. Silence no longer means consent.	Noted in Preamble 32 of the GDPR (EUR-Lex, 2019), the consent of data subjects should be presented by a clear affirmative action setting up a freely given, informed, specific and unambiguous indication of data subjects' agreement to their personal data processing, such as by an oral statement or by a written statement including electronic methods (Chirica, 2017).
Stronger enforcement	Twenty-eight data protection authorities, grouped by the European Data Protection Board, exercise the power to offer guidance and interpretation and use binding decisions in the case multiple EU countries with respect to the same case. The authorities enjoy harmonized powers and impose fines on organizations to a maximum of €20 million or four per cent of worldwide annual turnover.	The GDPR adopts a penalty system with heavy fines for those who commit data protection violations (Altmayer, 2018; Voss, 2017). Article 83 provides two stages of administrative fines depending on the circumstances of individual cases (Altmayer, 2018). The first stage, which is for infringements of some provisions including the obligations of the processor and the controller, and the monitoring body and certification body, can lead to administrative fines of up to €10 million or two per cent of the total worldwide annual turnover of the faulty organization, whichever is greater. The second stage is for more serious infringements such as violation of data subjects' rights and illegal transfers of personal data to a third-party country or international organizations, can lead to more massive fines up to €20 million or 4 per cent of the total global annual turnover of the organization, whichever is higher.

## Appendix B

### *A new era for data protection in the EU: What changes after May 2018. Adopted from European Commission (2019a)*



The Facebook/Cambridge Analytica revelations show the EU has made the right choice to propose and carry out an ambitious data protection reform through the General Data Protection Regulation (GDPR).


The General Data Protection Regulation rules will apply as of 25 May 2018. They will bring several improvements to deal with data protection violations in the future:

CLEAR LANGUAGE	
TODAY	TOMORROW
Often businesses explain their privacy policies in lengthy and complicated terms	Privacy policies will have to be written in a <b>clear, straightforward language</b>

CONSENT FROM USER	
TODAY	TOMORROW
Businesses sometimes assume that the user's silence means consent to data processing, or they hide a request for consent in long, legalistic, terms and conditions — that nobody reads	The user will need to give an <b>affirmative consent</b> before his/her data can be used by a business. Silence is no consent

(Continued)

2 A new era for data protection in the EU — What changes after May 2018




MORE TRANSPARENCY	
TODAY	TOMORROW
The user might not be informed when his/her data is transferred outside the EU	Businesses will need to <b>clearly inform</b> the user <b>about</b> such <b>transfers</b>
Sometimes businesses collect and process personal data for different purposes than for the reason initially announced without informing the user about it	Businesses will be able to collect and process data only for a <b>well-defined purpose</b> . They will have to inform the user about new purposes for processing
Businesses use algorithms to make decisions about the user based on his/her personal data (e.g. when applying for a loan); the user is often unaware about this	Businesses will have to <b>inform</b> the user <b>whether the decision is automated</b> and give him/her a possibility to contest it




(Continued)

A new era for data protection in the EU — What changes after May 2018 3



STRONGER RIGHTS	
TODAY	TOMORROW
Often businesses do not inform users when there is a data breach, for instance when the data is stolen	Businesses will have to <b>inform</b> users without delay in case of harmful data breach
Often the user cannot take his/her data from a business and move it to another competing service	The user will be able to <b>move</b> his/her <b>data</b> , for instance to another social media platform
It can be difficult for the user to get a copy of the data businesses keep about him/her	The user will have the right to <b>access</b> and get a copy of his/her data, a business has on him/her
It may be difficult for a user to have his/her data deleted	Users will have a clearly defined <b>“right to be forgotten”</b> (right to erasure), with clear safeguards



STRONGER ENFORCEMENT	
TODAY	TOMORROW
Data protection authorities have limited means and powers to cooperate	The <b>European Data Protection Board</b> grouping all 28 data protection authorities, will have the powers to provide <b>guidance</b> and <b>interpretation</b> and adopt <b>binding decisions</b> in case several EU countries are concerned by the same case
Authorities have no or limited fines at their disposal in case a business violates the rules	The 28 data protection authorities will have harmonised powers and will be able to <b>impose fines</b> to businesses up to 20 million EUR or 4% of a company's worldwide turnover

Visit the European Commission's online guidance on data protection reform — available in all EU languages:

[europea.eu/dataprotection](https://europea.eu/dataprotection)



## Appendix C

### Questionnaire items

#### Hypothesis-related questions

Construct	ID	Measurement Item	Source
Perceived technology			
Perceived usefulness	PU1	The website communicates the information I need in order to make purchase decisions.	Chen and Barnes (2007)
	PU2	The information on the website facilitates my decision-making processes.	
	PU3	The website is easy and functional for purchasing online.	
	PU4	The website can increase my shopping effectiveness, compared to other websites.	
Perceived ease-of-use	PE1	The website is easy to learn to use.	Chen and Barnes (2007)
	PE2	It is easy to get the website to do what I want.	
	PE3	My interactions with the website are understandable and clear. For example: the website mentions all tax, duties, shipping rates and any hidden costs to the customer before purchases are approved; it allows me to track my order status and update delivery address.	
Perceived risks			
Perceived privacy	PP1	The personal information that I provide to the website is secure.	Chen and Barnes (2007)
	PP2	The financial information I provide to the website is well protected.	
	PP3	The website will not use unsuitable methods to collect my personal data.	
	PP4	The website does not ask for irrelevant personal information.	
	PP5	The owner of the website does not use my personal information for other purposes.	
Perceived security	PS1	The customer's credit card information is unlikely to be disclosed through the website.	Mukherjee and Nath (2007)
	PS2	The security features used by the online retailer are up-to-date.	
	PS3	The website uses payment gateways for transactions (such as PayPal, AliPay) instead of using its own payment mechanisms (for example: you need to fill in your bank account information in a given table designed by the website itself).	
	PS4	The website has not been hacked in the past.	
Perceived third-party assurance	PTA1	I feel safe in buying products/services (or conducting business online) with the website because a third-party will protect me.	Bojang (2017)
	PTA2	I feel safe in buying (or conducting business online) from the website because of its statements of guarantees. For example: an international car	

		rental website (such as Hertz and Thrifty) is cooperating with a third party insurance company.	
	PTA3	I feel safe in buying (or conducting business online) from the website as it has a strong credit rating from third party companies.	
Perceived trustworthiness			
Perceived openness	PO1	The website clearly mentions its rules, regulations, policies and practices to the customers.	Mukherjee and Nath (2007)
	PO2	The website creates an open environment where customers can freely interact with other customers and communicate on the products and services of the website.	
Online customer trust	OCT1	The website operates its business in a highly dependable and reliable manner.	Chang and Fang (2013)
	OCT2	The website promotes customers' benefits as well as its own.	
	OCT3	The website does not engage in any kinds of exploitive and damaging behavior to customers.	
	OCT4	When browsing this site, I feel confident and assured.	
Online purchase intention	OPI1	I intend to (once again) make a purchase from the website.	Liu et al. (2017)
	OPI2	I would (once again) make a purchase from the website.	
	OPI3	I plan to (once again) make a purchase from the website in the future.	

### The GDPR-specific questions

Code	Item
Q1-Principle	If one of your favorite e-commerce websites implements the principles of the GDPR, would that increase your confidence and trust of using that website?
Q2-Principle	If the answer is Yes for the above question, would you please explain why? (Open-ended)
Q1-Fine	If you know the website is going to be faced with high fines and penalties for disobeying a data protection law, would that increase your confidence and trust of using that website?
Q2-Fine	If the answer is Yes for the above question, would you please explain why? (Open-ended)
Q1-Consent	If you are asked for your consent before your data can be used by the website, would that increase your confidence and trust of using that website?
Q2-Consent	If the answer is Yes for the above question, would you please explain why? (Open-ended)

## About the Authors

**Jingjing Zhang** graduated with her Master of Business Informatics degree from ICL Graduate Business School, Auckland, New Zealand in 2019. She has over ten years' experience in the public relations domain, focusing on both client service and organizational management. Her research interests include human behaviour and IS/human-computer interaction, information security and privacy, social media and business impact, IS/IT strategy, leadership, and governance. She completed a Postgraduate Diploma in Information Systems and Technology at the City University, London, in 2003. Jingjing Zhang is the corresponding author who can be contacted at [jzh1616@gmail.com](mailto:jzh1616@gmail.com)

**Dr Farkhondeh Hassandoust** is a lecturer in Business Information Systems, at Auckland University of Technology. Farkhondeh's research interests include IS use, information security and knowledge management. Her works have been published in *Pacific Asia Journal of the Association for Information Systems*, *Journal of Applied Research in Higher Education*, *Journal of Knowledge Management*, *Economics and Information Technology*, among others. She has also presented her works in international conferences such as European Conference on Information Systems, and Pacific Asia Conference on Information Systems. Her research has been supported by grants from Auckland University of Technology Vice-Chancellor's Doctoral Scholarship, and Internet New Zealand.

**Jocelyn E. Williams**, Associate Professor of Communication Studies and Academic Director of ICL Graduate Business School, Auckland, New Zealand, has been a communication researcher for over twenty years in areas including the knowledge gap hypothesis, information poverty, the Digital Divide, community informatics, community media and science communication. She combines her interests in leading and managing people in higher education with a love of qualitative research and writing, in an academic career that brings together her Master of Management (Massey University, 2001), PhD in Community Informatics (Massey University, 2010) and broad leadership experience including being President of the Australian and NZ Communication Association (ANZCA) to drive both higher education management and research achievements. Her papers have been presented at the Association of Internet Researchers conferences in Canada and the UK, and regularly at ANZCA, while her publications appear in journals including *Communication Research and Practice* and the *International Journal of Communication Ethics*, and in books such as *Social and Economic Effects of Community Wireless Networks and Infrastructures* (2013).