Taylor & Francis
Taylor & Francis Group

Behaviour & Information Technology

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/tbit20

General data protection regulation: a study on attitude and emotional empowerment

Davit Marikyan, Savvas Papagiannidis, Omer F. Rana & Rajiv Ranjan

BEHAVIOUR & INFORMATION TECHNOLOGY
https://doi.org/10.1080/0144929X.2023.2285341

Taylor & Francis
Taylor & Francis Group

OPEN ACCESS Check for updates

General data protection regulation: a study on attitude and emotional empowerment

Davit Marikyan[a], Savvas Papagiannidis[b], Omer F. Rana[c] and Rajiv Ranjan[d]

[a]School of Management, University of Bristol Business School, Bristol, UK; [b]Newcastle University Business School, Newcastle upon Tyne, UK; [c]School of Computer Science and Informatics, Cardiff University, Cardiff, UK; [d]School of Computing, Newcastle University, Newcastle upon Tyne, UK

ABSTRACT

Over the last few years, digitalisation has accelerated its pace, fuelling the creation of a massive amount of data. This has resulted in a need to introduce legal mechanisms to protect the privacy and security of data being exchanged between people and organisations. However, little is known about the individuals' perspective on such mechanisms. Given the gap in the literature, this research investigated the drivers and the implications of individuals' attitude towards GDPR compliance. To test the research model, structural equational modelling was employed using 540 responses. The result showed that perceived threat severity, self-efficacy and response efficacy determine a positive attitude towards GDPR compliance, which results in emotional empowerment. The findings contribute to the literature on legal privacy-preserving mechanisms, by providing a user's view on the coping and threat appraisal factors underpinning attitude and demonstrating the implications for driving confidence in control over personal data. The findings also contribute to the literature on protection motivation by demonstrating that attitude towards adaptive behaviour drives emotional empowerment. The study offers suggestions to policymakers on how to enhance public perception of the GDPR. The findings also provide guidelines for organisations on how to inform individuals' understanding of compliance with the legal framework.

ARTICLE HISTORY
Received 5 July 2022
Accepted 14 November 2023

KEYWORDS
Compliance behaviour; security; privacy; GDPR; satisfaction; digital economy

1. Introduction

The spread of digital technologies across all business sectors has led to the growing interconnectedness between people, internet-enabled devices and organisations, fuelling the rapid digitalisation of economic activities. Such activities reflect the changes in business processes, service delivery and communication with customers (Sturgeon 2021). The digital nature of transactions between users and companies has generated a vast amount of digital data, which has become a valuable source of competitive advantage for organisations (Hagiu and Wright 2020). Having consumer data can help organisations to tailor their services and products in accordance with consumer needs (Hagiu and Wright 2020). The role of data in organisational processes has become even more important after the outbreak of the pandemic, when governments introduced national and local lockdowns to reduce the potential spread of the virus (Carroll and Conboy 2020). In response to such measures, many businesses transferred their activities to online environments, in order to ensure business continuity (Papagiannidis, Harris, and Morton 2020; Venkatesh 2020). Rapid digitalisation, in turn, has fuelled concerns about data privacy (Pandey and Pal 2020; Urbaczewski and Lee 2020). Although privacy issues have long been on the agenda for policymakers and researchers (Kaapu and Tiainen 2009; Rohunen and Markkula 2019; Sørensen 2016), the recent growth in exchanges increases the importance of data protection mechanisms, such as the General Data Protection Regulation (GDPR), and their implications for people.

Introduced in the European Union in 2018, the objective of the GDPR is to give individuals an indisputable right to privacy and personal data protection (Goddard 2017; Presthus and Sønslien 2021; Van Ooijen and Vrabec 2019). Personal data refers to any piece of data that could be used to discern individuals, including but not limited to IP addresses, location data and digital fingerprinting (Goddard 2017; Tankard 2016). Digital fingerprints represent data, such as online behaviour, device configuration and browser information, generated about an individual when they visit

CONTACT Davit Marikyan davit.marikyan@bristol.ac.uk School of Management, University of Bristol, Queens Road, Bristol BS8 1QU, UK

websites (Bell 2011). The assurance that organisations comply with the GDPR – the belief that individuals' rights to privacy and personal data protection are acted upon by organisations – can strengthen confidence in control over personal data and potentially make individuals feel empowered (Strycharz, Ausloos, and Helberger 2020). However, perceived non-compliance of organisations with the GDPR can increase distrust towards them and impede individuals' data sharing behaviour (Karampela, Ouhbi, and Isomursu 2019). The unwillingness to participate in data sharing online can be an obstacle to the growth of e-commerce and the creation of agile information systems that can be instrumental for improving the quality and efficiency of services in different sectors, such as healthcare and transport (Hann et al. 2007; Karampela, Ouhbi, and Isomursu 2019; Nienaber et al. 2021). Therefore, the negative perception of privacy in data exchange could hold back digitalisation and its associated benefits. Given the increasing digital transformation of industries and services, and the participatory role of users in such processes (Karampela, Ouhbi, and Isomursu 2019), insight into individuals' perceptions of the regulation is needed (Pins et al. 2022). Specifically, it is important to understand the factors that underpin the attitude towards GDPR compliance. Furthermore, to ensure the wider collective effort towards the enforcement of GDPR practices in organisations, it is critical to understand how the perception of GPDR compliance influences an intrapersonal psychological state. Therefore, there is a need to explore individuals' emotional empowerment entailed by positive beliefs about GDPR compliance.

Researchers so far have extensively studied the legal and ethical aspects of the GDPR (De Hert et al. 2018; Forcier et al. 2019; Larrucea et al. 2020; Truong et al. 2019). There is sufficient evidence in the GDPR literature about the importance of privacy and security when using products/services (Balapour, Nikkhah, and Sabherwal 2020; Hasan, Shams, and Rahman 2021; Marabelli, Vaast, and Li 2021; Oghazi et al. 2020; Renwick and Gleasure 2021; Tolsdorf, Dehling, and Lo Iacono 2022) and the role of the regulation in attenuating privacy concerns (Paul, Scheibe, and Nilakanta 2020). However, despite discussions about the need to explore the GDPR from an individual's perspective (Paul, Scheibe, and Nilakanta 2020; Pins et al. 2022; Strycharz, Ausloos, and Helberger 2020; Van Ooijen and Vrabec 2019), user insights into the role and implementation of the GDPR are under-researched. The role of individuals' beliefs in relation to GDPR-compliant behaviour needs to be investigated by considering the privacy paradox dichotomy (Barth and de Jong 2017; Hann et al. 2007; Huberman, Adar, and Fine 2005; Kokolakis 2017). The privacy paradox is a privacy-compromising behaviour manifested by users, even though they express strong concerns about their data privacy and security (Barth and de Jong 2017; Kokolakis 2017). Users tend to assign value to privacy-protective behaviour (Hann et al. 2007; Huberman, Adar, and Fine 2005). If such behaviour comes at the cost of convenience or financial expenses, the motivation to engage in it decreases (Carrascal et al. 2013; Hann et al. 2007; Huberman, Adar, and Fine 2005). Hence, the role of cost-benefit analysis in privacy-compliant data exchange necessitates the evaluation of the cognitive factors underlying behaviour, which have not been examined to date. Secondly, although it has been argued that the GDPR empowers individuals to carry out transactions online without fear of having personal data being compromised (Strycharz, Ausloos, and Helberger 2020), little is known about how empowerment is manifested on an emotional level. Empowerment has mainly been investigated as an implied state reflecting the consumers' knowledge about the technical and legal measures. It enables individuals to protect their privacy online by restricting the use of personalised advertising or cookies (Strycharz et al. 2019; Strycharz et al. 2021). The practices that the regulation enforces (such as the right to modify, obtain and delete personal information after it has been collected), go beyond the management of access to data by third parties (Tikkinen-Piri, Rohunen, and Markkula 2018). As such, existing literature lacks evidence about the beliefs explaining the formation of the views on compliance with security-preserving regulatory frameworks, such as that of GDPR, and the emotional state of empowerment associated with such views.

To cover the above research gaps this study examines individuals' beliefs that underpin the perception and importance of protective behaviour ensured by the GDPR. To address this objective, first, we adopt Protection Motivation Theory to theorise and examine the role of the cognitive factors conducive to individuals' perceived threats and coping mechanisms. This helps us explore the impact of cognition on positive attitudes towards GDPR compliance. Evidence about the relationship between the cognitive factors associated with privacy and security threats and attitude is important for understanding the conditions that could potentially facilitate individuals' predisposition towards GDPR-compliant behaviour. Second, we investigate whether attitude leads to emotional empowerment. On the one hand, by testing this relationship, this study can provide insight into user perceptions of the degree to which the regulation makes people feel confident that they are in control of personal data exchanged online. On the other hand, such findings aim to shed light on the relationship between protection motivation and emotional empowerment.

The next section of the paper will provide a literature review on the GDPR and the rationale for developing the research model. This is followed by the hypothesis development section, which justifies the relationships between the identified variables. Then, the paper presents the methodology underpinning the study, outlines the results and discusses the findings. The paper concludes with theoretical and practical implications and suggestions for future research.

2. Literature review

GDPR is a legal privacy-assuring mechanism which was introduced to replace the 1995 Data Protection Directive (DPD) and provide guidelines to EU companies against the backdrop of the increasing role of Big Data in business (Zarsky 2016). The law aims to protect individuals' personal data following the principles of lawfulness, fairness, transparency, accuracy, accountability, confidentiality and integrity when it comes to data usage (Goddard 2017; Perera et al. 2019; Zaeem and Barber 2020). Organisations that are compliant with the GDPR should aim to minimise the amount of personal data collected to the amount which is required to provide the requested services. Consequently, the period of data storage should be limited to the purpose of data usage (Goddard 2017; Zaeem and Barber 2020). The goal of GDPR compliance is to improve individuals' confidence that their privacy is being respected and their personal data is being handled fairly (Perera et al. 2019; Zaeem and Barber 2020). Such confidence is ensured by giving individuals the rights to object to the collection of personal data, have access to personal information that was collected by third parties online, as well as rectify and delete the information after it was collected (Tikkinen-Piri, Rohunen, and Markkula 2018). Non-compliance by organisations can result in heavy fines, which can make it more difficult and costly for firms to operate in a GDPR environment (Albrecht 2016; Presthus and Sønslien 2021; Tankard 2016).

The importance of privacy preservation in view of the massive amounts of digital data created every day and the fact that the GDPR rules were formulated so recently has prompted the interest of researchers (Albrecht 2016; Larrucea et al. 2020; Tolsdorf, Dehling, and Lo Iacono 2022; Truong et al. 2019; Wachter, Mittelstadt, and Russell 2017; Wieringa et al. 2021). This interest has resulted in the development of research streams exploring the GDPR and its implications through mainly organisational, technical, legal and ethical lenses (De Hert et al. 2018; Goddard 2017; Wachter, Mittelstadt, and Russell 2017). For example, from an organisational perspective, studies have focused on the impact of the introduction of the GDPR on companies and the suggestions of best practice to anticipate and cope with the challenges posed by regulatory changes (Leite, Dos Santos, and Almeida 2022; Voss and Houser 2019; Ziegler, Evequoz, and Huamani 2019). On the one hand, it was found that the law had disrupted many areas of business practices (Leite, Dos Santos, and Almeida 2022). On the other hand, compliance with the regulation was found to provide a competitive advantage deriving from enhanced trust in the company (Voss and Houser 2019).

When viewed through a technical lens, the literature has offered insights into technological developments in different sectors and life domains to ensure compliance with data protection rules (Bassi et al. 2019; Mougiakou and Virvou 2017; Truong et al. 2019). On the one hand, researchers focused on system designs that would offer security in line with the regulation requirements (Campanile et al. 2021; Truong et al. 2019). For example, researchers proposed solutions that could process data in a fair and transparent way (Badii et al. 2020; Haque et al. 2021; Kounoudes and Kapitsaki 2020), restrict or minimise private data collection in unauthorised situations (Bassi et al. 2019; De Carvalho, Fantinato, and Eler 2020) and facilitate visual privacy protection (Asghar et al. 2019). On the other hand, the literature provides insights into the implications of the regulation for existing technologies. Specifically, studies have explored the role of the GDPR in enhancing the security of individuals' digital data (Mougiakou and Virvou 2017) and reducing the instances of online tracking (e.g. cookies) (Sanchez-Rola et al. 2019).

Studies in the legal domain have a strong focus on interpreting the GDPR, offering a comprehensive guide for GDPR compliance and suggesting improvements for policymakers (De Hert et al. 2018; Forcier et al. 2019; Leiser 2019). There is a growing awareness that there is a conflict between technology – e.g. the use of blockchains – and GDPR rules, such as the right to be forgotten, to delete and to edit personal data (Tatar, Gokce, and Nussbaum 2020). The implementation of these rules can be complicated when the data is in a blockchain, which is considered to be immutable and irreversible (Tatar, Gokce, and Nussbaum 2020). Also, there is a great deal of ambiguity when it comes to the applicability of the law to international organisations and the potential implications of its rules for firms (De Búrca 2020; Hustinx 2021; Kuner 2020). A sub-stream of the literature in the legal domain is concerned with the ethical side of the GDPR (Amram 2020; Larrucea et al. 2020; Rochel

2021; Vlahou et al. 2021). Although the legal framework embraces both jurisdictional and ethical standards about data processing (Amram 2020), the inseparability and the complementarity of ethics to the laws that regulate data use and processing are debated (Rochel 2021; Vlahou et al. 2021). Considering the lack of clarity about the relationship between ethics and law, the literature suggests that the principles of the GDPR can be interpreted from both perspectives (Rochel 2021; Vlahou et al. 2021).

As per above, there has been increasing interest in GDPR and ample research on GDPR-compliant technologies, legal and ethical implications. Still, the evidence about the individual's perspective on the legal framework is limited. Some studies have investigated the GDPR by looking into an individual's view on the regulation (Hartman et al. 2020; Mangini, Tal, and Moldovan 2020; Zhang, Wang, and Hsu 2020). The findings were not consistent. While it was shown that individuals were happy with specific GDPR rules, such as the right to be forgotten (Mangini, Tal, and Moldovan 2020), the public's view on the overall approach to managing data was negative (Hartman et al. 2020). However, the companies that voluntarily adhere to the laws that regulate data use and processing are perceived as trustworthy (Zhang, Wang, and Hsu 2020). Also, it was found that individuals are more willing to disclose personal information and have a lower perception of risks while engaging in online purchase transactions when they consider data protection laws to be effective (Paul, Scheibe, and Nilakanta 2020; Urbonavicius et al. 2021). Furthermore, despite the argued role of the GDPR in empowering individuals to enjoy their rights to personal data protection (Strycharz, Ausloos, and Helberger 2020), the impact of GDPR-compliant practices on people's emotional state of empowerment has not been examined.

The importance of emotional empowerment for this study stems from the research on psychological empowerment, suggesting that there are four empowerment states, namely relational, cognitive, emotional and behavioural (Peterson 2014; Peterson et al. 2021; Rodrigues, Menezes, and Ferreira 2018). Cognitive empowerment is also known as an interpersonal state, as it concerns the critical knowledge of the dynamics in the socio-political environment (Christens, Collura, and Tahir 2013; Zimmerman 1995). It is not only the understanding of the forces of the environment, but the resources and methods that are required to address the impact of the environment on oneself (Wilke and Speer 2011). In the non-social context, cognitive empowerment reflects an assessment of one's own behaviour, competence, self-efficacy, circumstances and behaviour consequences (Thomas and Velthouse 1990). Relational empowerment refers to interpersonal transactions helping individuals exercise their transformative power in the socio-political domain. Behavioural empowerment refers to individuals' actions directed at exerting influence over the social, political, economic and cultural conditions that affect the lives of communities. Emotional empowerment is the emotional state resulting from the awareness of personal ability to influence the conditions in the personal and socio-political contexts (Rodrigues, Menezes, and Ferreira 2018). When it comes to the GDPR application, cognitive empowerment reflects the knowledge of the responsibilities of organisations in ensuring data privacy, the consequences of the violation of the regulation and the rights of individuals whose data is collected. Such knowledge works as a motivational stimulus for attitude formation and behaviour change (Thomas and Velthouse 1990). Consequently, in the context of this study, individuals' knowledge of the benefits of the regulation for data privacy can affect the attitude towards GDPR compliance, rather than result from attitudinal change. Relational and behavioural empowerment are not pertinent for examining the psychological implications of GDPR compliance, because at the application stage, end-users have from limited or even no impact on how organisations adhere to regulations. In contrast, emotional empowerment refers to intra-personal psychological states, resulting from the assessment of the environment where behaviour takes place (Rodrigues, Menezes, and Ferreira 2018). Hence, the use of emotional empowerment makes it possible to explore feelings when individuals assess the regulatory framework when it comes to data privacy and security and realise their strength in controlling how their data is used by organisations.

The existing literature on GDPR has examined empowerment as an implied state. Researchers theorised the concept as individuals' knowledge about technology and legal rights, helping them make informed decisions as to whether to consent to or refuse the collection of personal data by third parties (Strycharz et al. 2019; Strycharz et al. 2021). Specifically, it was found that knowledge drives the evaluation of potential costs and benefits, and the subsequent intention to disclose personal information through personalised advertising and cookies (Strycharz et al. 2019; Strycharz et al. 2021). Such findings are helpful in explaining the instances when knowledge of behavioural costs and benefits can hinder or facilitate privacy-preserving behaviour. Still, the extant literature does not explain the motivation to engage in compliant behaviour, which includes a wider scope of practices than the consent to use cookies and personalised ads. Given the above evidence from extant research, the determinants of protective behaviour and the emotional implications of the regulation remain underexplored.

The attitude towards organisations' GDPR-compliant behaviour can be explained by the privacy-calculus research. This research postulates that privacy-related decisions are based on the premise that perceived benefits would outweigh perceived costs (Culnan and Armstrong 1999; Dinev and Hart 2006). Cost-benefit analysis underpins privacy-compliant and privacy-compromising behaviour (Barth and de Jong 2017; Carrascal et al. 2013; Hann et al. 2007; Huberman, Adar, and Fine 2005; Kokolakis 2017). Individuals may disclose personal information while engaging in transactions if they gain the benefits of cost-saving and convenience, even though it may be at the risk of the violation of online personal data use (Hann et al. 2007; Huberman, Adar, and Fine 2005; Kokolakis 2017). The intention to protect personal data privacy can prevail even if it might entail monetary costs (Egelman, Felt, and Wagner 2013). In a similar vein, organisations' practices directed at protecting individuals' data can be perceived positively by individuals if they believe that ensuring that organisations are compliant with the data law when it comes to data treatment is worth the effort. The belief that one has to spend significant time, money and effort to ensure that organisations do not breach data privacy would probably undermine the value of a company's privacy-protective behaviour. In turn, the threats of personal data misuse and the effectiveness of privacy-protective behaviour are expected to positively affect the evaluation of that behaviour. Given the above, the evaluation of potential threats and the benefits of protective mechanisms eliminating these threats could be decisive factors shaping the attitude towards GDPR-compliant practices.

Therefore, the focus of this paper is on examining the cognitive factors facilitating a positive attitude towards GDPR-compliant behaviour and the resulting feeling of empowerment. By adopting the selected approach, we aim to gain a deeper insight into the determinants that may explain individuals' perceptions of GDPR-compliant behaviour and the implications of perceptions for an individual's psychological state. The following section will provide a justification for the proposed hypotheses in the research model.

3. Theoretical foundation and hypothesis development

The study uses Protection Motivation Theory as a theoretical foundation to investigate an individual's attitude towards GDPR compliance and the following feeling of emotional empowerment. The theory has been helpful in guiding prior studies on individuals' motivation to engage in security and privacy-preserving behaviour through the employment of technologies with an extra layer of security and adherence to privacy policies (Herath et al. 2014; Hsieh and Lai 2020; Ifinedo 2012; Marikyan et al. 2022; Menard, Bott, and Crossler 2017; Orazi and Johnston 2020).

Protection Motivation Theory posits that individuals' attitudes to compliance behaviours, actual behaviour and behavioural intention are facilitated by the perception of threat vulnerability, threat severity, response efficacy and self-efficacy, and hindered by the perception of response cost (Boss et al. 2015; Rogers 1983; Wu 2020). Early research applying Protection Motivation Theory suggested that the effects on protection motivation are mediated by two cognitive mechanisms, namely threat appraisal and coping appraisal (Boss et al. 2015; Floyd, Prentice-Dunn, and Rogers 2000), which led to some scholars treating appraisal factors as second-order constructs (e.g. Byrd et al. 2023). However, a wide body of research adopts a simplified conceptualisation of protection motivation which omits mediating cognitive appraisal factors. Researchers in that stream of literature examine protective attitudes and behaviour as directly predicted by the perceptions of response efficacy, self-efficacy, threat vulnerability, threat severity and response cost, suggesting that these perceptions denote threat and coping appraisal cognitions (Lee 2011; Menard, Bott, and Crossler 2017; Vance, Siponen, and Pahnila 2012).

Threat appraisal happens when individuals evaluate one's own vulnerability to threat and threat severity (Boss et al. 2015; Rogers 1983). Perceived threat vulnerability concerns the appraisal of the likelihood of the threatening event happening (Ifinedo 2012). In the context of this research, perceived threat vulnerability captures an individual's assessment of the likelihood of their personal data being compromised. Protection Motivation Theory postulates that individuals' vulnerability to potential danger triggers the motivation to engage in protective behaviour (Boss et al. 2015; Chen et al. 2020; Rogers 1983). However, empirical evidence has demonstrated that the relationship between perceived threat vulnerability and behaviour is not consistently significant across studies (Boss et al. 2015; Ifinedo 2012; Lee 2011; Vance, Siponen, and Pahnila 2012). For instance, the research on users' intention to back up data did not show a significant role of perceived threat vulnerability (Boss et al. 2015; Crossler 2010). A study examining the adoption of anti-plagiarism software established an opposite finding. It was found that the assessment of personal susceptibility to threat was a significant driver to anti-spyware adoption and compliance with information systems security policy (Chenoweth, Minch, and Gattiker 2009; Ifinedo 2012; Lee 2011). Perceived threat severity concerns an individual's perception of how harmful the threat of counter protective behaviour might be (Boss et al. 2015; Chen et al. 2020; Rogers 1983). In relation to GDPR practices, perceived threat severity refers to an individual's evaluation of the severity of harm that privacy intrusion and data protection breaches might cause. In the scenario of malicious treatment of data, potential harm is considered to be severe enough to motivate individuals to engage in protective behaviour. Such behaviour may involve the installation of anti-spyware (Chenoweth, Minch, and Gattiker 2009), the purchase of anti-plagiarism software (Lee 2011), compliance with security policies (Vance, Siponen, and Pahnila 2012), intention to take protective measures (De Kimpe et al. 2022) and other activities helping diminish the potential threat. Given the above, the importance of personal privacy and the increasing security threats, we hypothesise the following.

> Hypothesis 1: (a) Perceived threat vulnerability and (b) perceived threat severity positively relate to attitude towards GDPR compliance.

Following Protection Motivation Theory, coping appraisal refers to individuals' consideration of their own ability to cope with the consequences of a threat (Woon, Tan, and Low 2005). Coping appraisal captures the assessment of self-efficacy, response efficacy and response cost (Ifinedo 2012). Self-efficacy reflects individuals' beliefs that they are able to fulfil behaviour to achieve certain things or events (Bandura 1977; Bandura 1982). Individuals' confidence in being able to cope with the task increases their motivation to commence it (Boss et al. 2015; Rippetoe and Rogers 1987). For example, it was found that individuals who scored high on the perceived self-efficacy scale tend to abide by IS security policies (Vance, Siponen, and Pahnila 2012), install anti-spyware software (Lee and Larsen 2009) and back up personal data (Crossler 2010). The relationship between self-efficacy and behaviour is explained by the role of personal capabilities in amplifying the effectiveness of one's own behaviour (Rogers 1983). When it comes to GDPR practices, self-efficacy reflects the individuals' perception of personal ability to ensure that organisations getting hold of their data would treat it in compliance with the data law. The perception of self-efficacy, in turn, strengthens the belief that the GDPR rules are effective. Response efficacy reflects an individual's belief that undertaking protective behaviour will result in benefits (Rogers 1983). In the context of this research, response efficacy refers to individuals' beliefs that adherence to the GDPR will result in rewards. Individuals who believe that complying with security and data protection regulations will help reduce the instances of data violation tend to follow this law (Crossler 2010; Herath et al. 2014; Ifinedo 2012). The response cost factor captures the perception of the costs that the engagement with protective behaviour will entail (Ifinedo 2012). Response cost diminishes the motivation to commence the protective behaviour (Chenoweth, Minch, and Gattiker 2009; Lee and Larsen 2009). When individuals believe that the implementation of IS security measures might be difficult, time-consuming or costly, their motivation to undertake such measures decreases (Chenoweth, Minch, and Gattiker 2009; Lee 2011; Woon, Tan, and Low 2005). Given the above evidence, we postulate that:

> Hypothesis 2: (a) Self-efficacy and (b) response efficacy positively relate to attitude towards GDPR compliance. (c) Response cost negatively relates to attitude towards GDPR compliance.

This study proposes that attitude towards GDPR compliance positively relates to individuals' feelings of emotional empowerment. Attitude is an individual's evaluative judgement (Schwarz 2007) and has been considered as a proxy for behaviour and employed to investigate technology adoption, adaptive and maladaptive use of technology amongst other activities (Tamilmani et al. 2020b; Tamilmani, Rana, and Dwivedi 2020a; Porter and Donthu 2006; Ratchford and Ratchford 2021; Wu 2020). In the information management domain, attitude is an individual's salient beliefs about using technology and the assessment of the benefits related to its use (Karahanna, Straub, and Chervany 1999). In the context of this research, attitude is an individual's overall assessment of the benefits related to GDPR adherence when processing third-party data. Emotional empowerment is a type of psychological empowerment state. Psychological empowerment can be described as individuals' beliefs that they have access to resources, rights and knowledge providing the capabilities to control a situation, and giving individuals the possibility to participate in the attainment of goals (Maton 2008; Zimmerman 1995). The feeling of emotional empowerment captures an intra-personal psychological state arising from the realisation of personal abilities to affect things and events in personal and socio-political contexts (Peterson et al. 2021). Emotional empowerment reflects how people perceive themselves in terms of domain-specific control, self-efficacy and competence (Zimmerman 1995). The concept of empowerment is critical in legal scholarship, as

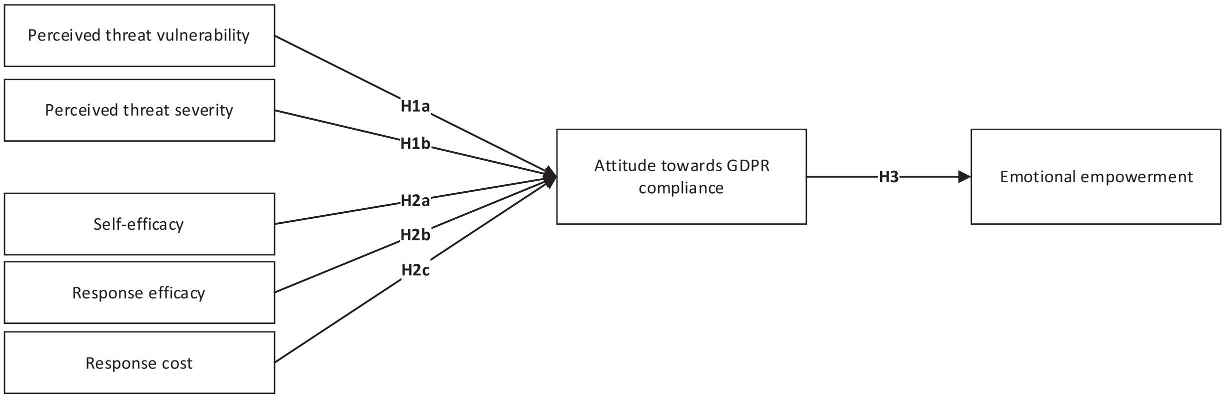
Perceived threat vulnerability
Perceived threat severity
Self-efficacy
Response efficacy
Response cost
H1a
H1b
H2a
H2b
H2c
Attitude towards GDPR compliance
H3
Emotional empowerment

Figure 1. Attitude towards GDPR compliance.

it encourages the involvement of citizens in addressing communal issues and rights (Beckers 2018; Christens, Collura, and Tahir 2013; Mak and Terryn 2020). When it comes to GDPR-compliant behaviour, individuals may feel emotionally empowered for two reasons. First, the regulation gives individuals the ability to control data online, providing information about the purpose for which data is collected and how it is processed. Knowledge about the technical aspect of data processing and the awareness of the effectiveness of legal intervention in ensuring data protection reflect the confidence in protective behaviour (Strycharz et al. 2021; Strycharz et al. 2019). Second, the legal mechanism ensures that a breach of data protection laws by organisations incurs high costs (Tankard 2016; Albrecht, 2016; Presthus and Sønslien 2021). This implies a higher likelihood that the regulatory framework will be followed by organisations, thus increasing confidence in the outcome of protective measures and personal abilities to influence protective behaviour (Strycharz et al. 2021; Strycharz et al. 2019). Consequently, the perception that the GDPR protects individuals' rights to fair data treatment can enhance one's perceived control over personal data and induce associated positive emotions. Therefore, the third hypothesis states that:

> Hypothesis 3: Individuals' attitude towards GDPR compliance is positively related to emotional empowerment.

The relationships between coping appraisal, threat appraisal, attitude and empowerment are presented in Figure 1.

4. Methodology

4.1. Data collection

Given the objectives of this study, we employed a cross-sectional research design. Before launching the data collection, first we consulted with a researcher in the law discipline, focusing on data protection and public consent, and a researcher involved in technology development, focusing on information systems compliant with privacy-preserving regulations. The objective of the consultation was to ensure that the identified constructs and their adaptation were relevant for a legal security-preserving framework and confirm that the objective knowledge scale represented a good measure of the knowledge of the regulation among the general population. After consultation with the experts, a pilot survey was conducted to generate feedback about the comprehensiveness of the survey, the clarity of the questions and the survey design and structure. The pilot questionnaire was distributed to 20 fellow researchers and Prolific users. Upon the completion of the pilot study and incorporating suggestions/feedback about the wording of the questions provided by the respondents, we embarked on the full-scale data collection. The final questionnaire contained three parts. The first part was the introduction to the survey explaining the purpose of the data collection and including a consent form. We made it explicit in the introduction block of the questionnaire that participation was anonymous, voluntary and respondents could decline or terminate the survey at any point in time. The second part included questions to test the research model, while the third part aimed to collect socio-demographic information about the respondents. For the data collection, we used a convenience sampling method to recruit respondents from a consumer panel in the UK. Access to the sample was provided by Prolific, an independent research company, which distributed a URL to the study among the consumer panel. The use of a research company to collect data enabled quick access to a sample of UK citizens who are eligible to participate in the study, and increased the likelihood of accurate responses due to the incentives offered to respondents for each valid response. As a result, 564

Table 1. The profile of the respondents.

Demographic characteristic	Type	Frequency ($n = 540$)	Percentage
Age	18–24	157	29.1%
	25–35	140	25.9%
	35–44	87	16.1%
	45–54	86	15.9%
	55–64	50	9.3%
	65 or older	20	3.7%
Education	Completed some high school	31	5.7%
	Completed some college (GSCE/ASA/A-level)	221	40.9%
	Bachelor's degree	202	37.4%
	Master's degree	72	13.3%
	Other advanced degree beyond a Master's degree	4	0.7%
	PhD	10	1.9%
Gender	Male	226	41.9%
	Female	314	58.1%
Importance (Privacy)	Low	18	3.3%
	Neutral	18	3.3%
	High	504	93.3%
Expertise	Low	266	49.3%
	Medium	23	4.3%
	High	251	46.5%
Control over personal data	Low	213	39.4%
	Medium	37	6.9%
	High	290	53.7%
Fear (of privacy intrusion)	Low	102	18.9%
	Medium	29	5.4%
	High	409	75.7%
Objective knowledge	Low	43	8.0%
	Medium	161	29.8%
	High	336	62.2%

questionnaires were distributed, out of which 540 were returned with complete and valid responses (Table 1). The majority of the respondents were aged between 18 and 35 (55%) and had completed some college or attained a Bachelor's degree (78.3%). In terms of gender, the sample was relatively balanced with 41.9% of men compared to 58.1% of women. A predominant number of respondents considered the importance of privacy to be high (93.3%) and had a strong fear of privacy intrusion (75.7%). While the percentage of respondents with high expertise (46.5%) is similar to the percentage of those with low expertise (49.3%), most of the respondents considered themselves to have a medium and high level of objective knowledge about the GDPR (92%).

4.2. Measurement

To ensure the validity of the measures we employed scales from prior literature (Table 2) and the measurement items of seven constructs were anchored on a 7-point Likert scale. The points ranged from 1 'strongly disagree' to 7 'strongly agree'. The scales were adapted to fit the context and the objectives of the study. For the socio-demographic profile, we measured individuals' objective knowledge about the GDPR. The scale for this study was developed using an approach employed by other scholars (Manika, Gregory-Smith, and Papagiannidis 2018). The questions about the objective knowledge were gleaned from the GDPR literature and checked by GDPR experts (Appendix). The GDPR experts were two researchers who had been involved in the research on the regulations around digital technology and the development of privacy-preserving information systems compliant with data protection laws. They validated the accuracy of the questions and answers, as well as the relevance of the questions for measuring the objective knowledge of the general public, who do not have professional experience in law. The questions were intended to measure the respondents' knowledge of the responsibilities of organisations in ensuring data privacy, their responses to privacy violation, the rights of individuals whose data is collected and the role of individuals in adhering to the GDPR.

5. Results

5.1. Data analysis

Given the objective of the study to test the research model, covariance-based structural equation modelling (CB-SEM) was used as a data analysis approach. Prior to conducting the analysis, multivariate analysis assumptions were tested. First, the collinearity diagnostics using SPSS were conducted to eliminate the possibility of multicollinearity between independent variables in the model (Tabachnick, Fidell, and Ullman 2007). The tolerance coefficients were >0.1, while the VIF values were <10, which indicated that the variables were not highly correlated (Thompson et al. 2017). Second, to identify outliers and their effect on the model, the Mahalanobis Distances and Cook's Distance coefficients were extracted. Residual statistics showed that there were cases with standardised residuals falling beyond the suggested range between −3.3 and +3.3. However, since Cook's Distances were not above 1, it was considered that the outliers did not have an affect on the results of the analysis (Tabachnick, Fidell, and Ullman 2007). Apart from the analysis of outliers in SPSS, we also checked Mahalanobis Distances in Amos. Ten cases with significant farthest distances from the centroid were identified. To reconfirm that they did not influence the accuracy of the analysis output, the model was tested with and without the identified outliers, which demonstrated that there were no differences in the effect sizes and p-values of the tested relationships. Third, to test the linearity, normality and homoscedasticity of the data, Normal P-Plot and

Table 2. Measurement items of constructs.

Measurement Item	Loading	*α*
Perceived threat severity (Vance, Siponen, and Pahnila 2012; Ifinedo 2012)		0.768
Threats to the security of my personal data can be harmful	0.710	
I view access to my private data without my permission as harmful	0.798	
Having my private data accessed by someone without my consent is a serious problem for me	0.797	
Perceived threat vulnerability (Johnston and Warkentin 2010; Ifinedo 2012)		0.880
I can fall victim to data breach	0.811	
The risk of illegal access to my personal data can be high	0.808	
My personal data can be compromised	0.871	
My personal data can be vulnerable to breaches	0.753	
Response efficacy (Vance, Siponen, and Pahnila 2012; Woon, Tan, and Low 2005)		0.910
GDPR is important when it comes to protecting my data because …		
It would reduce the likelihood of personal data breaches.	0.850	
The instances of data breaches would be fewer	0.864	
It would help avoid threats to my personal data	0.858	
It would be an effective way of deterring potential data breaches	0.823	
Self-efficacy (Woon, Tan, and Low 2005)		0.834
Ensuring that organisations that hold my personal data comply with GDPR …		
Would help protect my personal data	0.803	
Would reduce the risk of data breaches	0.895	
Response Cost (Vance, Siponen, and Pahnila 2012)		0.859
Ensuring that organisations that hold my personal data comply with GDPR …		
Would incur overhead costs	0.724	
Would require investment of effort	0.852	
Would be time-consuming	0.885	
Attitude towards GDPR compliance (Elliott, Armitage, and Baughan 2007)		0.940
Compliance with GDPR is …		
A good practice	0.822	
Important	0.841	
Beneficial	0.857	
Positive	0.897	
Valuable	0.874	
Wise	0.826	
Emotional empowerment (Peterson et al. 2021)		0.892
The rules that GDPR imposes on organisations …		
Make me aware of my strength as an owner of data	0.823	
Make me feel in control of my own data	0.879	
Make me feel confident	0.825	
Make me speak up for my rights about the usage of my data	0.763	

Scatterplot were inspected. All values were distributed linearly along the diagonal line on the Normal P-Plot and around '0' on the Scatterplot. That enabled us to conclude the normality and linearity of data and proceed to the analysis of the measurement and structural models (Tabachnick, Fidell, and Ullman 2007).

SPSS v.26 and SPSS-AMOS v.26 were employed to examine the reliability and validity of the adopted measurements and to explore the hypothesised paths. Overall, the analysis procedures followed two steps. The first step was to carry out confirmatory factor analysis to eliminate the possibility of validity and reliability issues. To ensure the measurement model's validity and reliability, we tested the Cronbach's Alpha values, factor loadings, construct reliability, average variance extracted, and CFA model fit indices. As a result of the validity, reliability and model fit analyses, the values were above the acceptable threshold, which is >0.9 for CFI, <0.07 for RMSEA, >0.7 for CR, factor loadings and Cronbach Alpha coefficients, and >0.5 for AVE (Hair et al. 2014). Specifically, the measurement model fit indices were: χ^2 (278) = 632.700, CMIN/DF = 2.276, CFI 0.962, RMSEA = 0.049. Since the sample size was large, χ^2 was significant as expected (Hair et al. 2014). Table 2 presents the factor loadings and Cronbach Alpha coefficients. One item from the self-efficacy scale was deleted as the factor loading was <0.5, which is below the suggested threshold (Hair et al. 2014). The results of convergent and discriminant validity analysis, along with CR and AVE values are provided in Table 3. The diagonal figures in Table 3 represent the square root of the average variance extracted (AVE), while the figures below represent the between-constructs correlations. Discriminant validity was established, as the diagonal figures are higher than the between-constructs correlations. In addition, as all data were collected from the same source, we made sure that common method variance would not affect the results. Three post-hoc tests were employed to reject the possibility of a common method bias, suggested by Podsakoff et al. (2003). A Harman's single-factor test showed that one factor explained 30.7% of the variance, the inclusion of a latent variable demonstrated 17% of the variance, while the test using a latent factor and a

Table 3. Convergent and discriminant validity test.

	C.R	AVE	1	2	3	4	5	6	7
Response cost	0.862	0.678	0.823						
Perceived threat severity	0.813	0.592	0.047	0.769					
Perceived threat vulnerability	0.885	0.659	0.235**	0.342**	0.812				
Attitude towards GDPR compliance	0.941	0.728	−0.013	0.303**	0.167**	0.853			
Response efficacy	0.912	0.721	−0.041	0.211**	0.053	0.458**	0.849		
Self-efficacy	0.839	0.723	−0.088*	0.163**	0.025	0.471**	0.618**	0.850	
Empowerment	0.894	0.678	−0.075	0.172**	0.078	0.377**	0.447**	0.402**	0.824

Note: significant at *p*-value: ***<.001, **<.01, *<.05, ns > .05.

marker variable showed a variance of 16%. All of the values were below the acceptable threshold (Podsakoff et al. 2003).

5.2. Structural model analysis

The second step of the structural equation modelling analysis was checking the structural model fit indices and the analysis of the hypothesised paths. Following the guidelines by Hair et al. (2014), the structural model fit indices were satisfactory, with χ^2 having a significant *p*-value, CFI > 0.9 and RMSEA < 0.07 (χ^2 (283) = 698.930, CMIN/DF = 2.470, CFI = 0.956, RMSEA = 0.052). Given the result of fit testing, we embarked on checking the proposed relationships. The results of the structural model analysis are presented in Table 4, showing that all the proposed hypotheses were supported except H1a and H2c. The model explains 37% of the variance in attitude towards GDPR compliance and 18% of the variance in empowerment.

6. Discussion

The analysis of the factors underpinning individuals' attitude towards GDPR compliance showed that when it comes to threat appraisal the role of perceived threat vulnerability is not significant. This indicates that individuals do not feel vulnerable to potential security and privacy breaches, which goes against the principles of Protection Motivation Theory (Rogers 1983) and the literature examining compliance behaviour (Lee 2011; Ifinedo 2012). However, there is empirical evidence that this factor has an insignificant effect on individuals' behaviour (Vance, Siponen, and Pahnila 2012; Crossler and Bélanger 2014; Tsai et al. 2016; Crossler et al. 2014; Chen and Yeh 2017). A plausible explanation could be that individuals think that government and organisations ensure their privacy and can provide compensation in the case of a breach. Hence users feel sufficiently protected. On the other hand, perceived threat severity was found to have a positive significant relationship with attitude towards GDPR compliance. The results are in line with research examining human behaviour in relation to privacy-insurance mechanisms (Mousavi et al. 2020; Vance, Siponen, and Pahnila 2012; Lee 2011; De Kimpe et al. 2022). Considering the non-significant effect of threat vulnerability, individuals might recognise the severity of the degree to which potential security and privacy breaches could affect them. However, as they have high objective knowledge about GDPR, they might believe that the compliance with the regulatory framework reduces the risk of such threats arising.

When it comes to coping factors, all factors but response cost were found to have significant relationships with attitude towards GDPR compliance. The positive path between self-efficacy and attitude indicates that individuals are confident that organisations complying with the GDPR can protect their personal data and reduce the chances of data breaches. This is logical as the demographic profile of the respondents shows that the majority of them had high objective knowledge. That means that they were aware of the benefits of the law and how organisations can act to protect individuals' right to privacy. Therefore, the respondents believed that ensuring that organisations processing personal data comply with the GDPR principles can help protect personal data. That belief, in turn, improves individuals' attitudes towards GDPR-compliant behaviour. This finding is in line with the principles of

Table 4. The results of the structural model analysis.

H	Path	Standardised coef. (*β*)	*t*-test, *p*-value
H1a	Perceived threat vulnerability → Attitude towards GDPR compliance	0.070	1.516^{ns}
H1b	Perceived threat severity → Attitude towards GDPR compliance	0.213	4.435***
H2a	Self-efficacy → Attitude towards GDPR compliance	0.323	4.933***
H2b	Response efficacy → Attitude towards GDPR compliance	0.220	3.495***
H2c	Response cost → Attitude towards GDPR compliance	0.002	0.057^{ns}
H3	Attitude towards GDPR compliance → Empowerment	0.431	9.274***

Note: significant at *p*-value: ***<.001, **<.01, *<.05, ns > .05.

Protection Motivation Theory and related research examining security compliant behaviour (Lee 2011; Ifinedo 2012; Crossler 2010; Mousavi et al. 2020; Marikyan et al. 2022). Similarly, the positive relationship between response efficacy and attitude (H2b) is consistent with evidence confirming the role of this factor in motivating security practices (Lee 2011; Ifinedo 2012; Crossler 2010; Tsai et al. 2016). Attitude towards GDPR compliance is determined by the perception that adherence to the GDPR by organisations can eliminate security and privacy issues. Given that the respondents hold high objective knowledge about the GDPR, the results could mean that the understanding of the data-preserving mechanism increases the confidence in the effectiveness of the regulation and, in turn, attitude towards the practices it promotes. The insignificant path between response cost and attitude contradicts the principles of Protection Motivation Theory (Floyd, Prentice-Dunn, and Rogers 2000), although there have been conflicting results about the effect of the construct on protective behaviour (Ifinedo 2012; Boss et al. 2015; Crossler 2010; Crossler and Bélanger 2014). The perceived cost of compliance with the data-preserving regulation does not diminish individuals' predisposition towards that behaviour. A potential explanation could be that individuals know that GDPR compliance is mandatory, which gives organisations no choice but to follow the law. An alternative interpretation could be that respondents believe that companies' compliance with the GDPR is important, which overshadows the costs associated with the measures that need to be taken to ensure the privacy and security of data. Such an interpretation can be supported by the privacy-calculus research (Culnan and Armstrong 1999; Dinev and Hart 2006), suggesting that the perceived costs are lower than the benefits of the behaviour and thus irrelevant when it comes to the formation of the attitude towards it.

As far as the path between attitude towards GDPR compliance and emotional empowerment is concerned, the analysis showed that the two constructs positively correlate. This is the first empirical evidence confirming the relationship between the perception of GDPR-compliant practices and empowerment. A positive attitude towards GDPR-compliant practices reflects individuals' beliefs that the law is an effective measure to protect personal data, enabling individuals to refuse access to data, see how it is used and provide a means to manage, rectify and delete data after it has been collected (Maton 2008; Peterson et al. 2021; Guchait, Kim, and Namasivayam 2012). The belief that the GDPR can help avoid data privacy and security issues increases individuals' confidence, which is associated with a positive psychological and emotional state (Boshoff and Leong 1998; Boshoff 1997). An affective state stems from an individual's realisation of personal capabilities to control the situation and achieve their goals (Maton 2008; Zimmerman 1995). This finding complements the existing literature about the potentially empowering role of the knowledge of technical/legal underpinnings of GDPR compliance and the effectiveness of the legal framework in privacy-preserving behaviour (Strycharz et al. 2021; Strycharz et al. 2019).

6.1. Theoretical and practical contributions

This paper makes several contributions to the literature. Firstly, it contributes to the literature on legal data protection mechanisms. The study responds to a call to explore the user perspective on the regulatory framework (GDPR), which has been under-researched so far (Van Ooijen and Vrabec 2019; Strycharz, Ausloos, and Helberger 2020). The results of the analysis of the research model shed light on how the beliefs induced by the fear of data privacy and security risks correlate with the individual's perception of the privacy-preserving regulatory framework. This finding is important for understanding the factors that can enhance a positive attitude towards GDPR compliance and be associated with a feeling of emotional empowerment.

Second, the findings of the paper extend the knowledge on protection motivation. This study provides evidence about the emotional state following motivation to engage in adaptive behaviour, which was made possible by examining the relationship between attitude towards GDPR compliance and empowerment. While some prior studies suggested that cognitive appraisal factors play a role when a person feels empowered (Strycharz et al. 2021; Strycharz et al. 2019), the variable has not been empirically measured. The investigation of empowerment is important in the context of protective behaviour for two reasons. First, empowerment captures the strength of individual agency in protective behaviour (Zimmerman 1995), while coping and threat factors reflect the evaluation of the efficacy of protective measures (Rogers 1983). Hence, the confirmed role of empowerment enables us to understand whether perceived coping efficacy and threat strength can translate into personal control over the consequences of threat-inducing actions in a specific domain. Second, the confirmation of the significance of the psychological state has particular importance for examining the motivations for adaptive behaviour, because empowerment reflects a striving for control and the awareness of a personal participatory role and skills in problem-solving (Zimmerman 1995).

Third, the study contributes to the literature on information systems management. The established relationships between fear-induced beliefs and a positive attitude towards GDPR compliance serve as empirical evidence about the drivers of the use of technologies enhancing individuals' privacy and data security. This evidence is timely, considering growing research directed towards the development of privacy-preserving systems and the exploration of the factors underpinning the adoption of such technology (Truong et al. 2019; Mora et al. 2021; Lumor et al. 2021). The findings about the coping and threat appraisal variables correlating with attitude towards GDPR compliance provide an understanding of the cognitive factors that increase the likelihood of the acceptance of privacy-preserving technologies.

From a practice perspective, this research provides several implications for organisations and policymakers. Given that threat and coping mechanisms determine attitude towards GDPR compliance, open discussion events about the implications of GDPR compliance would encourage an understanding of the benefits of the regulation for different stakeholders. To communicate to the public that they will not fall victim to data misuse, organisations need to ensure that the way in which they treat data is communicated to their stakeholders. The information can be communicated through dedicated pages on firms' websites with a description of the purposes and the types of data that the company collects, processes and stores. To increase individuals' awareness of personal data use, consent forms need to be prompted before individuals' data can be collected. Also, this study can guide policymakers. To enhance trust in the law, which contributes to the perceived effectiveness of GDPR practices, policymakers need to improve the general public's awareness of the benefits of the regulatory framework. The perception of the importance and the effectiveness of the law can be improved by increasing the involvement of individuals in learning the impact of GDPR compliance through multiple channels, such as live consultancy chats, workshops and podcasts.

7. Conclusion, limitations and future research suggestions

To address the research gaps in the current literature lacking the individuals' perspectives on the legal security-preserving framework, this study examined individuals' attitudes towards GDPR compliance and the individuals' perception of empowerment. To meet the objective, the research model was developed analysing the cognitive antecedents of attitude and the resulting feeling of empowerment.

This study has some limitations that future research can build upon. Since the objective of this study revolved around a specific data law, in the future, researchers could investigate individuals' views on privacy-preserving legal frameworks that are practised outside of the GDPR zone. An international and intercultural perspective is important, as people from different cultures could have a dissimilar perception of legal and governmental interventions and privacy in general (Wu et al. 2012; Cram, Proudfoot, and D'arcy 2017). Second, this study focused on the psychological implications of GDPR application in organisations, which defined the focus on the emotional type of empowerment. Future research could investigate the role of individuals in the formation of the regulation and explore the consequences of a positive attitude towards the regulation in terms of behavioural and relational empowerment. Third, given that threat vulnerability was not significant, future studies could explore the reasons that would explain such beliefs. A possible approach might be to examine the effect of threat vulnerability in two conditions: when individuals have had and have not had prior experience of data protection issues. It is plausible that a prior negative experience of private data misuse increases individuals' beliefs that a similar situation could happen. Fourth, while this study investigated the factors underpinning the attitude towards and experience of GDPR practices, future studies could investigate the psychological factors determining non-compliant behaviour. This approach could shed light on the potential inhibitors of the legal framework implementation. Fifth, future research can extrapolate the findings of the insignificant role of response cost. Studies could examine empirically as to whether the factor is not significant due to the compliance with the GDPR being mandatory or whether the importance of law overshadows any costs associated with the actions that need to be taken to ensure compliance.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This project has been funded by the Engineering and Physical Sciences Research Council (EPSRC): PACE: Privacy-Aware Cloud Ecosystems (Project Reference: EP/R033293/1).

References

Albrecht, J. P. 2016. "How the GDPR Will Change the World." *European Data Protection Law Review* 2 (3): 287. https://doi.org/10.21552/EDPL/2016/3/4.

Amram, D. 2020. "Building up the "Accountable Ulysses" Model. The Impact of GDPR and National Implementations, Ethics, and Health-Data Research: Comparative Remarks." *Computer Law & Security Review* 37: 105413. https://doi.org/10.1016/j.clsr.2020.105413

Asghar, M. N., N. Kanwal, B. Lee, M. Fleury, M. Herbst, and Y. Qiao. 2019. "Visual Surveillance Within the EU General Data Protection Regulation: A Technology Perspective." *IEEE Access* 7: 111709–111726. https://doi.org/10.1109/ACCESS.2019.2934226

Badii, C., P. Bellini, A. Difino, and P. Nesi. 2020. "Smart City IoT Platform Respecting GDPR Privacy and Security Aspects." *IEEE Access* 8: 23601–23623. https://doi.org/10.1109/ACCESS.2020.2968741

Balapour, A., H. R. Nikkhah, and R. Sabherwal. 2020. "Mobile Application Security: Role of Perceived Privacy as the Predictor of Security Perceptions." *International Journal of Information Management* 52: 102063. https://doi.org/10.1016/j.ijinfomgt.2019.102063

Bandura, A. 1977. "Self-efficacy: Toward a Unifying Theory of Behavioral Change." *Psychological Review* 84 (2): 191–215. https://doi.org/10.1037/0033-295X.84.2.191.

Bandura, A. 1982. "Self-efficacy Mechanism in Human Agency." *American Psychologist* 37 (2): 122. https://doi.org/10.1037/0003-066X.37.2.122.

Barth, S., and M. D. de Jong. 2017. "The Privacy Paradox–Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behavior–A Systematic Literature Review." *Telematics and Informatics* 34 (7): 1038–1058. https://doi.org/10.1016/j.tele.2017.04.013

Bassi, E., N. Bloise, J. Dirutigliano, G. P. Fici, U. Pagallo, S. Primatesta, and F. Quagliotti. 2019. "The Design of GDPR-Abiding Drones Through Flight Operation Maps: A Win–Win Approach to Data Protection, Aerospace Engineering, and Risk Management." *Minds and Machines* 29 (4): 579–601. https://doi.org/10.1007/s11023-019-09511-9

Beckers, A. 2018. "Environmental Protection Meets Consumer Sales." *European Review of Contract Law* 14 (2): 157–189. https://doi.org/10.1515/ercl-2018-1009.

Bell, G. B. 2011. "Digital Whistleblowing in Restricted Environments." *Journal of Digital Information* 12 (3): 1–14.

Boshoff, C. 1997. "An Experimental Study of Service Recovery Options." *International Journal of Service Industry Management* 8 (2): 110–130. https://doi.org/10.1108/09564239710166245.

Boshoff, C., and J. Leong. 1998. "Empowerment, Attribution and Apologising as Dimensions of Service Recovery: An Experimental Study." *International Journal of Service Industry Management* 9 (1): 24–47. https://doi.org/10.1108/09564239810199932.

Boss, S. R., D. F. Galletta, P. B. Lowry, G. D. Moody, and P. Polak. 2015. "What do Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors." *MIS Quarterly* 39 (4): 837–864.

Byrd, K., A. Fan, E. Her, Y. Liu, S. Leitch, and B. Almanza. 2023. "Restaurant Patronage During the COVID-19 Pandemic and the Protection Motivation Theory: Influence of Consumers' Socio-Demographic, Situational, and Psychographic Factors." *Journal of Foodservice Business Research* 26 (2): 247–275. https://doi.org/10.1080/15378020.2021.2006036

Campanile, L., M. Iacono, F. Marulli, and M. Mastroianni. 2021. "Designing a GDPR Compliant Blockchain-Based IoV Distributed Information Tracking System." *Information Processing & Management* 58 (3): 102511. https://doi.org/10.1016/j.ipm.2021.102511

Carrascal, J. P., C. Riederer, V. Erramilli, M. Cherubini, and R. De Oliveira. 2013. "Your Browsing Behavior for a Big Mac: Economics of Personal Information Online." In *Proceedings of the 22nd International Conference on World Wide Web*, 189–200.

Carroll, N., and K. Conboy. 2020. "Normalising the "New Normal": Changing Tech-Driven Work Practices Under Pandemic Time Pressure." *International Journal of Information Management* 55: 102186. https://doi.org/10.1016/j.ijinfomgt.2020.102186

Chen, K.-Y., and C.-F. Yeh. 2017. "Factors Affecting Adoption of Smart Meters in the Post-Fukushima era in Taiwan: An Extended Protection Motivation Theory Perspective." *Behaviour & Information Technology* 36 (9): 955–969. https://doi.org/10.1080/0144929X.2017.1317363

Chen, C., K. Z. Zhang, X. Gong, M. K. Lee, and Y. Wang. 2020. "Decreasing the Problematic use of an Information System: An Empirical Investigation of Smartphone Game Players." *Information Systems Journal* 30 (3): 492–534. https://doi.org/10.1111/isj.12264

Chenoweth, T., R. Minch, and T. Gattiker. 2009. "Application of Protection Motivation Theory to Adoption of Protective Technologies." In *2009 42nd Hawaii International Conference on System Sciences*, 1–10. IEEE.

Christens, B. D., J. J. Collura, and F. Tahir. 2013. "Critical Hopefulness: A Person-Centered Analysis of the Intersection of Cognitive and Emotional Empowerment." *American Journal of Community Psychology* 52 (1-2): 170–184. https://doi.org/10.1007/s10464-013-9586-2

Cram, W. A., J. G. Proudfoot, and J. D'arcy. 2017. "Organizational Information Security Policies: A Review and Research Framework." *European Journal of Information Systems* 26 (6): 605–641. https://doi.org/10.1057/s41303-017-0059-9

Crossler, R. E. 2010. "Protection Motivation Theory: Understanding Determinants to Backing Up Personal Data." In *2010 43rd Hawaii International Conference on System Sciences*, 1–10. IEEE.

Crossler, R., and F. Bélanger. 2014. "An Extended Perspective on Individual Security Behaviors: Protection Motivation Theory and a Unified Security Practices (USP) Instrument." *ACM SIGMIS Database: The DATABASE for Advances in Information Systems* 45 (4): 51–71. https://doi.org/10.1145/2691517.2691521

Crossler, R. E., J. H. Long, T. M. Loraas, and B. S. Trinkle. 2014. "Understanding Compliance with Bring Your own Device Policies Utilizing Protection Motivation Theory: Bridging the Intention-Behavior gap." *Journal of Information Systems* 28 (1): 209–226. https://doi.org/10.2308/isys-50704

Culnan, M. J., and P. K. Armstrong. 1999. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation." *Organization Science* 10 (1): 104–115. https://doi.org/10.1287/orsc.10.1.104

De Búrca, G. 2020. "Introduction to the Symposium on the GDPR and International Law." *American Journal of International Law* 114 (1): 1–4. https://doi.org/10.1017/ajil.2019.70

De Carvalho, L. G., M. Fantinato, and M. M. Eler. 2020. “Security Requirements Identification and Prioritization for Smart Toys.” *Electronic Commerce Research and Applications* 41: 100972. https://doi.org/10.1016/j.elerap.2020.100972

De Hert, P., V. Papakonstantinou, G. Malgieri, L. Beslay, and I. Sanchez. 2018. “The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services.” *Computer Law & Security Review* 34 (2): 193–203. https://doi.org/10.1016/j.clsr.2017.10.003

De Kimpe, Lies, Michel Walrave, Pieter Verdegem, and Koen Ponnet. 2022. “What We Think We Know About Cybersecurity: An Investigation of the Relationship Between Perceived Knowledge, Internet Trust, and Protection Motivation in a Cybercrime Context.” *Behaviour & Information Technology* 41 (8): 1796–1808. http://dx.doi.org/10.1080/0144929X.2021.1905066.

Dinev, T., and P. Hart. 2006. “An Extended Privacy Calculus Model for e-Commerce Transactions.” *Information Systems Research* 17 (1): 61–80. https://doi.org/10.1287/isre.1060.0080

Egelman, S., A. P. Felt, and D. Wagner. 2013. “Choice Architecture and Smartphone Privacy: There’s a Price for That.” In *The Economics of Information Security and Privacy*, edited by R. Böhme, 211–236. Berlin: Springer.

Elliott, M. A., C. J. Armitage, and C. J. Baughan. 2007. “Using the Theory of Planned Behaviour to Predict Observed Driving Behaviour.” *British Journal of Social Psychology* 46 (1): 69–90. https://doi.org/10.1348/014466605X90801

Floyd, D. L., S. Prentice-Dunn, and R. W. Rogers. 2000. “A Meta-Analysis of Research on Protection Motivation Theory.” *Journal of Applied Social Psychology* 30 (2): 407–429. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x

Forcier, M. B., H. Gallois, S. Mullan, and Y. Joly. 2019. “Integrating Artificial Intelligence Into Health Care Through Data Access: Can the GDPR act as a Beacon for Policymakers?” *Journal of Law and the Biosciences* 6 (1): 317. https://doi.org/10.1093/jlb/lsz013

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. https://doi.org/10.2501/IJMR-2017-050

Guchait, P., M. G. Kim, and K. Namasivayam. 2012. “Error Management at Different Organizational Levels–Frontline, Manager, and Company.” *International Journal of Hospitality Management* 31 (1): 12–22. https://doi.org/10.1016/j.ijhm.2011.04.007

Hagiu, A., and J. Wright. 2020. “When Data Creates Competitive Advantage.” *Harvard Business Review* 98: 94–101.

Hair, J. F., W. C. Black, B. J. Babin, and R. E. Anderson. 2014. *Multivariate Data Analysis: Pearson New International Edition*. Essex: Pearson.

Hann, I.-H., K.-L. Hui, S.-Y. T. Lee, and I. P. Png. 2007. “Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach.” *Journal of Management Information Systems* 24 (2): 13–42. https://doi.org/10.2753/MIS0742-1222240202

Haque, A. B., A. N. Islam, S. Hyrynsalmi, B. Naqvi, and K. Smolander. 2021. “GDPR Compliant Blockchains–A Systematic Literature Review.” *IEEE Access* 9: 50593–50606. https://doi.org/10.1109/ACCESS.2021.3069877.

Hartman, T., H. Kennedy, R. Steedman, and R. Jones. 2020. “Public Perceptions of Good Data Management: Findings from a UK-Based Survey.” *Big Data & Society* 7 (1): 2053951720935616. https://doi.org/10.1177/2053951720935616

Hasan, R., R. Shams, and M. Rahman. 2021. “Consumer Trust and Perceived Risk for Voice-Controlled Artificial Intelligence: The Case of Siri.” *Journal of Business Research* 131: 591–597. https://doi.org/10.1016/j.jbusres.2020.12.012

Herath, T., R. Chen, J. Wang, K. Banjara, J. Wilbur, and H. R. Rao. 2014. “Security Services as Coping Mechanisms: An Investigation Into User Intention to Adopt an Email Authentication Service.” *Information Systems Journal* 24 (1): 61–84. https://doi.org/10.1111/j.1365-2575.2012.00420.x

Hsieh, P.-J., and H.-M. Lai. 2020. “Exploring Peoples Intentions to use the Health Passbook in Self-Management: An Extension of the Technology Acceptance and Health Behavior Theoretical Perspectives in Health Literacy.” *Technological Forecasting and Social Change* 161: 120328. https://doi.org/10.1016/j.techfore.2020.120328

Huberman, B. A., E. Adar, and L. R. Fine. 2005. “Valuating Privacy.” *IEEE Security & Privacy* 3 (5): 22–25. https://doi.org/10.1109/MSP.2005.137

Hustinx, P. 2021. “Data Protection and International Organizations: A Dialogue Between EU law and International law.” *International Data Privacy Law* 11 (2): 77–80. https://doi.org/10.1093/idpl/ipab015.

Ifinedo, P. 2012. “Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory.” *Computers & Security* 31 (1): 83–95. https://doi.org/10.1016/j.cose.2011.10.007

Johnston, A. C., and M. Warkentin. 2010. “Fear Appeals and Information Security Behaviors: An Empirical Study.” *MIS Quarterly* 34 (3): 549–566. https://doi.org/10.2307/25750691.

Kaapu, T., and T. Tiainen. 2009. “Consumers’ Views on Privacy in E-Commerce.” *Scandinavian Journal of Information Systems* 21: 1.

Karahanna, E., D. W. Straub, and N. L. Chervany. 1999. “Information Technology Adoption Across Time: A Cross-Sectional Comparison of pre-Adoption and Post-Adoption Beliefs.” *MIS Quarterly* 23 (2): 183–213. https://doi.org/10.2307/249751.

Karampela, M., S. Ouhbi, and M. Isomursu. 2019. “Exploring Users’ Willingness to Share Their Health and Personal Data Under the Prism of the New GDPR: Implications in Healthcare.” In *2019 41st Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, 6509–6512. IEEE.

Kokolakis, S. 2017. “Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon.” *Computers & Security* 64: 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Kounoudes, A. D., and G. M. Kapitsaki. 2020. “A Mapping of IoT User-Centric Privacy Preserving Approaches to the GDPR.” *Internet of Things* 11: 100179. https://doi.org/10.1016/j.iot.2020.100179

Kuner, C. 2020. “The GDPR and International Organizations.” *American Journal of International Law* 114: 15–19.

Larrucea, X., M. Moffie, S. Asaf, and I. Santamaria. 2020. "Towards a GDPR Compliant way to Secure European Cross Border Healthcare Industry 4.0." *Computer Standards & Interfaces* 69: 103408. https://doi.org/10.1016/j.csi.2019.103408

Lee, Y. 2011. "Understanding Anti-Plagiarism Software Adoption: An Extended Protection Motivation Theory Perspective." *Decision Support Systems* 50 (2): 361–369. https://doi.org/10.1016/j.dss.2010.07.009

Lee, Y., and K. R. Larsen. 2009. "Threat or Coping Appraisal: Determinants of SMB Executives' Decision to Adopt Anti-Malware Software." *European Journal of Information Systems* 18 (2): 177–187. https://doi.org/10.1057/ejis.2009.11

Leiser, M. 2019. "Regulating Computational Propaganda: Lessons from International law." *Cambridge International Law Journal* 8 (2): 218–240. https://doi.org/10.4337/cilj.2019.02.03

Leite, L., D. R. Dos Santos, and F. Almeida. 2022. "The Impact of General Data Protection Regulation on Software Engineering Practices." *Information & Computer Security* 30 (1): 79–96. https://doi.org/10.1108/ICS-03-2020-0043.

Lumor, T., M. Pulkkinen, A. Hirvonen, and P. Neittaanmäki. 2021. "Creating the Socio-Technical Context Needed to Derive Benefits from Big Data Initiatives in Healthcare." *Scandinavian Journal of Information Systems* 33: 1.

Mak, V., and E. Terryn. 2020. "Circular Economy and Consumer Protection: The Consumer as a Citizen and the Limits of Empowerment Through Consumer law." *Journal of Consumer Policy* 43 (1): 227–248. https://doi.org/10.1007/s10603-019-09435-y

Mangini, V., I. Tal, and A.-N. Moldovan. 2020. "An Empirical Study on the Impact of GDPR and Right to Be Forgotten-Organisations and Users Perspective." In *Proceedings of the 15th International Conference on Availability, Reliability and Security*, 1–9.

Manika, D., D. Gregory-Smith, and S. Papagiannidis. 2018. "The Influence of Prior Knowledge Structures on Website Attitudes and Behavioral Intentions." *Computers in Human Behavior* 78: 44–58. https://doi.org/10.1016/j.chb.2017.09.024

Marabelli, M., E. Vaast, and J. L. Li. 2021. "Preventing the Digital Scars of COVID-19." *European Journal of Information Systems* 30 (2): 176–192. https://doi.org/10.1080/0960085X.2020.1863752

Marikyan, D., S. Papagiannidis, O. F. Rana, and R. Ranjan. 2022. "Blockchain Adoption: A Study of Cognitive Factors Underpinning Decision Making." *Computers in Human Behavior* 131: 107207. https://doi.org/10.1016/j.chb.2022.107207.

Maton, K. I. 2008. "Empowering Community Settings: Agents of Individual Development, Community Betterment, and Positive Social Change." *American Journal of Community Psychology* 41 (1–2): 4–21. https://doi.org/10.1007/s10464-007-9148-6

Menard, P., G. J. Bott, and R. E. Crossler. 2017. "User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory." *Journal of Management Information Systems* 34 (4): 1203–1230. https://doi.org/10.1080/07421222.2017.1394083

Mora, H., J. C. Mendoza-Tello, E. G. Varela-Guzmán, and J. Szymanski. 2021. "Blockchain Technologies to Address Smart City and Society Challenges." *Computers in Human Behavior* 122: 106854. https://doi.org/10.1016/j.chb.2021.106854

Mougiakou, E., and M. Virvou. 2017. "Based on GDPR Privacy in UML: Case of e-Learning Program." In *2017 8th International Conference on Information, Intelligence, Systems & Applications (IISA)*, 1–8. IEEE.

Mousavi, R., R. Chen, D. J. Kim, and K. Chen. 2020. "Effectiveness of Privacy Assurance Mechanisms in Users' Privacy Protection on Social Networking Sites from the Perspective of Protection Motivation Theory." *Decision Support Systems* 135: 113323. https://doi.org/10.1016/j.dss.2020.113323

Nienaber, A.-M., S. Spundflasch, A. Soares, and A. Woodcock. 2021. "Distrust as a Hazard for Future Sustainable Mobility Planning. Rethinking Employees' Vulnerability When Introducing New Information and Communication Technologies in Local Authorities." *International Journal of Human–Computer Interaction* 37 (4): 390–401. https://doi.org/10.1080/10447318.2020.1860547

Oghazi, P., R. Schultheiss, K. Chirumalla, N. P. Kalmer, and F. F. Rad. 2020. "User Self-Disclosure on Social Network Sites: A Cross-Cultural Study on Facebook's Privacy Concepts." *Journal of Business Research* 112: 531–540. https://doi.org/10.1016/j.jbusres.2019.12.006

Orazi, D. C., and A. C. Johnston. 2020. "Running Field Experiments Using Facebook Split Test." *Journal of Business Research* 118: 189–198. https://doi.org/10.1016/j.jbusres.2020.06.053

Pandey, N., and A. Pal. 2020. "Impact of Digital Surge During Covid-19 Pandemic: A Viewpoint on Research and Practice." *International Journal of Information Management* 55: 102171. https://doi.org/10.1016/j.ijinfomgt.2020.102171

Papagiannidis, S., J. Harris, and D. Morton. 2020. "WHO led the Digital Transformation of Your Company? A Reflection of IT Related Challenges During the Pandemic." *International Journal of Information Management* 55: 102166. https://doi.org/10.1016/j.ijinfomgt.2020.102166

Paul, C., K. Scheibe, and S. Nilakanta. 2020. "Privacy Concerns Regarding Wearable IoT Devices: How It Is Influenced by GDPR?" Proceedings of the 53rd Hawaii International Conference on System Sciences.

Perera, H., W. Hussain, D. Mougouei, R. A. Shams, A. Nurwidyantoro, and J. Whittle. 2019. "Towards Integrating Human Values into Software: Mapping Principles and Rights of GDPR to Values." In *2019 IEEE 27th International Requirements Engineering Conference (RE)*, 404–409. IEEE.

Peterson, N. A. 2014. "Empowerment Theory: Clarifying the Nature of Higher-Order Multidimensional Constructs." *American Journal of Community Psychology* 53 (1-2): 96–108. https://doi.org/10.1007/s10464-013-9624-0

Peterson, N. A., D. T. Lardier, K. G. Powell, E. Mankopf, M. Rashid, C. M. Morton, and S. Borys. 2021. "Psychometric Properties of a Recovery Empowerment Scale: Testing Emotional, Cognitive, Behavioral, and Relational Domains." *Journal of Community Psychology* 49 (7): 2874–2891. https://doi.org/10.1002/jcop.22592.

Pins, D., T. Jakobi, G. Stevens, F. Alizadeh, and J. Krüger. 2022. “Finding, Getting and Understanding: The User Journey for the GDPR’S Right to Access.” *Behaviour & Information Technology* 41 (10): 2174–2200. https://doi.org/10.1080/0144929X.2022.2074894.

Podsakoff, P. M., S. B. Mackenzie, J.-Y. Lee, and N. P. Podsakoff. 2003. “Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies.” *Journal of Applied Psychology* 88 (5): 879–903. https://doi.org/10.1037/0021-9010.88.5.879.

Porter, C. E., and N. Donthu. 2006. “Using the Technology Acceptance Model to Explain how Attitudes Determine Internet Usage: The Role of Perceived Access Barriers and Demographics.” *Journal of Business Research* 59 (9): 999–1007. https://doi.org/10.1016/j.jbusres.2006.06.003

Presthus, W., and K. F. Sønslien. 2021. “An analysis of violations and sanctions following the GDPR.” *International Journal of Information Systems and Project Management* 9 (1): 38–53. https://doi.org/10.12821/ijispm090102.

Ratchford, M., and B. T. Ratchford. 2021. “A Cross-Category Analysis of Dispositional Drivers of Technology Adoption.” *Journal of Business Research* 127: 300–311. https://doi.org/10.1016/j.jbusres.2021.01.037

Renwick, R., and R. Gleasure. 2021. “Those who Control the Code Control the Rules: How Different Perspectives of Privacy are Being Written Into the Code of Blockchain Systems.” *Journal of Information Technology* 36 (1): 16–38. https://doi.org/10.1177/0268396220944406

Rippetoe, P. A., and R. W. Rogers. 1987. “Effects of Components of Protection-Motivation Theory on Adaptive and Maladaptive Coping with a Health Threat.” *Journal of Personality and Social Psychology* 52 (3): 596–604. https://doi.org/10.1037/0022-3514.52.3.596.

Rochel, J. 2021. “Ethics in the GDPR: A Blueprint for Applied Legal Theory.” *International Data Privacy Law* 11 (2): 209–223. https://doi.org/10.1093/idpl/ipab007.

Rodrigues, M., I. Menezes, and P. D. Ferreira. 2018. “Validating the Formative Nature of Psychological Empowerment Construct: Testing Cognitive, Emotional, Behavioral, and Relational Empowerment Components.” *Journal of Community Psychology* 46 (1): 58–78. https://doi.org/10.1002/jcop.21916

Rogers, R. W. 1983. “Cognitive and Psychological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation.” In *Social Psychophysiology: A Sourcebook*, edited by J. T. Cacioppo and R. Petty, 153–176. New York: Guilford Press.

Rohunen, A., and J. Markkula. 2019. “On the Road–Listening to Data Subjects’ Personal Mobility Data Privacy Concerns.” *Behaviour & Information Technology* 38 (5): 486–502. https://doi.org/10.1080/0144929X.2018.1540658

Sanchez-Rola, I., M. Dell’amico, P. Kotzias, D. Balzarotti, L. Bilge, P.-A. Vervier, and I. Santos. 2019. “Can I Opt Out Yet? GDPR and the Global Illusion of Cookie Control.” In *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*, 340–351.

Schwarz, N. 2007. “Attitude Construction: Evaluation in Context.” *Social Cognition* 25 (5): 638–656. https://doi.org/10.1521/soco.2007.25.5.638

Sørensen, C. 2016. “The Curse of the Smart Machine? Digitalisation and the Children of the Mainframe.” *Scandinavian Journal of Information Systems* 28: 3.

Strycharz, J., J. Ausloos, and N. Helberger. 2020. “Data Protection or Data Frustration? Individual Perceptions and Attitudes Towards the GDPR.” *European Data Protection Law Review* 6: 407–421. https://doi.org/10.21552/edpl/2020/3/10.

Strycharz, J., E. Smit, N. Helberger, and G. Van Noort. 2021. “No to Cookies: Empowering Impact of Technical and Legal Knowledge on Rejecting Tracking Cookies.” *Computers in Human Behavior* 120: 106750. https://doi.org/10.1016/j.chb.2021.106750

Strycharz, J., G. Van Noort, E. Smit, and N. Helberger. 2019. “Protective Behavior Against Personalized Ads: Motivation to Turn Personalization off.” *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 13 (2). https://doi.org/10.5817/CP2019-2-1.

Sturgeon, T. J. 2021. “Upgrading Strategies for the Digital Economy.” *Global Strategy Journal* 11 (1): 34–57. https://doi.org/10.1002/gsj.1364

Tabachnick, B. G., L. S. Fidell, and J. B. Ullman. 2007. *Using Multivariate Statistics*. Boston, MA: Pearson.

Tamilmani, K., N. P. Rana, and Y. K. Dwivedi. 2020a. “Consumer Acceptance and use of Information Technology: A Meta-Analytic Evaluation of UTAUT2.” *Information Systems Frontiers* 23: 987–1005. https://doi.org/10.1007/s10796-020-10007-6.

Tamilmani, K., N. P. Rana, R. Nunkoo, V. Raghavan, and Y. K. Dwivedi. 2020b. “Indian Travellers’ Adoption of Airbnb Platform.” *Information Systems Frontiers* 24: 77–96. https://doi.org/10.1007/s10796-020-10060-1.

Tankard, C. 2016. “What the GDPR Means for Businesses.” *Network Security* 2016 (6): 5–8. https://doi.org/10.1016/S1353-4858(16)30056-3

Tatar, U., Y. Gokce, and B. Nussbaum. 2020. “Law Versus Technology: Blockchain, GDPR, and Tough Tradeoffs.” . *Computer Law & Security Review* 38: 105454. https://doi.org/10.1016/j.clsr.2020.105454

Thomas, K. W., and B. A. Velthouse. 1990. “Cognitive Elements of Empowerment: An “Interpretive” Model of Intrinsic Task Motivation.” *Academy of Management Review* 15: 666–681.

Thompson, C. G., R. S. Kim, A. M. Aloe, and B. J. Becker. 2017. “Extracting the Variance Inflation Factor and Other Multicollinearity Diagnostics from Typical Regression Results.” *Basic and Applied Social Psychology* 39 (2): 81–90. https://doi.org/10.1080/01973533.2016.1277529

Tikkinen-Piri, C., A. Rohunen, and J. Markkula. 2018. “EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies.” *Computer Law & Security Review* 34 (1): 134–153. https://doi.org/10.1016/j.clsr.2017.05.015

Tolsdorf, J., F. Dehling, and L. Lo Iacono. 2022. “Data Cart – Designing a Tool for the GDPR-Compliant Handling of Personal Data by Employees.” *Behaviour & Information Technology* 41 (10): 2084–2119. https://doi.org/10.1080/0144929X.2022.2069596.

Truong, N. B., K. Sun, G. M. Lee, and Y. Guo. 2019. “Gdpr-compliant Personal Data Management: A Blockchain-Based Solution.” *IEEE Transactions on Information Forensics and Security* 15: 1746–1761. https://doi.org/10.1109/TIFS.2019.2948287.

Tsai, H.-Y. S., M. Jiang, S. Alhabash, R. Larose, N. J. Rifon, and S. R. Cotten. 2016. "Understanding Online Safety Behaviors: A Protection Motivation Theory Perspective." *Computers & Security* 59: 138–150. https://doi.org/10.1016/j.cose.2016.02.009

Urbaczewski, A., and Y. J. Lee. 2020. "Information Technology and the Pandemic: A Preliminary Multinational Analysis of the Impact of Mobile Tracking Technology on the COVID-19 Contagion Control." *European Journal of Information Systems* 29 (4): 405–414. https://doi.org/10.1080/0960085X.2020.1802358

Urbonavicius, S., M. Degutis, I. Zimaitis, V. Kaduskeviciute, and V. Skare. 2021. "From Social Networking to Willingness to Disclose Personal Data When Shopping Online: Modelling in the Context of Social Exchange Theory." *Journal of Business Research* 136: 76–85. https://doi.org/10.1016/j.jbusres.2021.07.031

Vance, A., M. Siponen, and S. Pahnila. 2012. "Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory." *Information & Management* 49 (3-4): 190–198. https://doi.org/10.1016/j.im.2012.04.002

Van Ooijen, I., and H. U. Vrabec. 2019. "Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective." *Journal of Consumer Policy* 42 (1): 91–107. https://doi.org/10.1007/s10603-018-9399-7

Venkatesh, V. 2020. "Impacts of COVID-19: A Research Agenda to Support People in Their Fight." *International Journal of Information Management* 55: 102197. https://doi.org/10.1016/j.ijinfomgt.2020.102197

Vlahou, A., D. Hallinan, R. Apweiler, A. Argiles, J. Beige, A. Benigni, R. Bischoff, P. C. Black, F. Boehm, and J. Céraline. 2021. "Data Sharing Under the General Data Protection Regulation: Time to Harmonize Law and Research Ethics?" *Hypertension* 77 (4): 1029–1035. https://doi.org/10.1161/HYPERTENSIONAHA.120.16340

Voss, W. G., and K. A. Houser. 2019. "Personal Data and the GDPR: Providing a Competitive Advantage for US Companies." *American Business Law Journal* 56 (2): 287–344. https://doi.org/10.1111/ablj.12139

Wachter, S., B. Mittelstadt, and C. Russell. 2017. "Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR." *Harvard Journal of Law & Technology* 31: 841.

Wieringa, J., P. Kannan, X. Ma, T. Reutterer, H. Risselada, and B. Skiera. 2021. "Data Analytics in a Privacy-Concerned World." *Journal of Business Research* 122: 915–925. https://doi.org/10.1016/j.jbusres.2019.05.005

Wilke, L. A., and P. W. Speer. 2011. "The Mediating Influence of Organizational Characteristics in the Relationship Between Organizational Type and Relational Power: An Extension of Psychological Empowerment Research." *Journal of Community Psychology* 39 (8): 972–986. https://doi.org/10.1002/jcop.20484

Woon, I., G.-W. Tan, and R. Low. 2005. "A Protection Motivation Theory Approach to Home Wireless Security." In *ICIS 2005 Proceedings*, 31.

Wu, D. 2020. "Empirical Study of Knowledge Withholding in Cyberspace: Integrating Protection Motivation Theory and Theory of Reasoned Behavior." *Computers in Human Behavior* 105: 106229. https://doi.org/10.1016/j.chb.2019.106229

Wu, K.-W., S. Y. Huang, D. C. Yen, and I. Popova. 2012. "The Effect of Online Privacy Policy on Consumer Privacy Concern and Trust." *Computers in Human Behavior* 28 (3): 889–897. https://doi.org/10.1016/j.chb.2011.12.008

Zaeem, R. N., and K. S. Barber. 2020. "The Effect of the GDPR on Privacy Policies: Recent Progress and Future Promise." *ACM Transactions on Management Information Systems (TMIS)* 12: 1–20.

Zarsky, T. Z. 2016. "Incompatible: The GDPR in the Age of Big Data." *Seton Hall Law Review* 47: 995.

Zhang, Y., T. Wang, and C. Hsu. 2020. "The Effects of Voluntary GDPR Adoption and the Readability of Privacy Statements on Customers' Information Disclosure Intention and Trust." *Journal of Intellectual Capital* 21 (2): 145–163. https://doi.org/10.1108/JIC-05-2019-0113.

Ziegler, S., E. Evequoz, and A. M. P. Huamani. 2019. "The Impact of the European General Data Protection Regulation (GDPR) on Future Data Business Models: Toward a New Paradigm and Business Opportunities." In *Digital Business Models*, edited by A. Aagaard. London Borough of Camden: Springer.

Zimmerman, M. A. 1995. "Psychological Empowerment: Issues and Illustrations." *American Journal of Community Psychology* 23 (5): 581–599. https://doi.org/10.1007/BF02506983

Appendix. Objective Knowledge Scale

Statements: Under the General Data Protection Regulation (GDPR) …	True	False	I do not know
Individuals have a right to be informed about the collection and use of their personal data			
Individuals have a right to be informed about the purposes for which their personal data have been collected			
The party who collects personal information should provide privacy notice prior to collection			
Individuals have a right to access and receive a copy of their personal data and other supplementary information			
Organisations should respond to the inquiries of individuals about their personal data within 1 month			
GDPR ensures that individuals have a right to rectify or complete inaccurate personal data			
In case of data breach, organisations have maximum 48 h to report it			
Consent to collect data should be obtained before collecting personal data			
Any information relating to an identified or identifiable person is defined as 'personal data'			
UK-EU citizens and all bodies processing their data are subject to GDPR			
The party who uses AI (artificial intelligence) to collect personal data should explain the purpose of using it before collecting data			