Enabling horizontal monitoring by applying a privacy by design framework

D.G.C. (Dennis) Teuben, dennis.teuben@student.hu.nl
HU University of Applied Science, Master of Informatics, P.O. Box 182, 3500 AD Utrecht, The Netherlands.
21 June 2021

ABSTRACT
The value of data, such as personal data, is almost impossible to overestimate. The protection of this personal data as part of private life by Article 8 of the European Convention on Human Rights (ECHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR) highlights its importance. In a democratic society, people should be able to trust that organizations handle personal data carefully and that over privacy protection is effective and decisive. This research examines whether a privacy control framework (PCF) can be designed based on privacy by design (PbD) principles. While conducting the research, we found it important to make these overarching principles concrete and practical. In addition, we investigated whether a new and more modern form of, a so-called horizontal monitoring (HM) relationship, could be achieved with this PCF. This method of comes from the tax industry and improves the effectiveness and efficiency of. As a result, the supervisory body can make better use of their often limited capacity and, for example, assume their role as an authority and advisory body. This qualitative research was carried out based on both a literature review and interviews, with the data collected leading to the conclusion described. An important finding from the study is that although horizontal monitoring leads to more effective and efficient, it requires significant effort from both parties. A horizontal relationship also requires capacity and energy.

KEYWORDS: privacy, privacy by design (PbD), horizontal monitoring (HM), Dutch Data Protection Authority

1. INTRODUCTION

People regularly see failures in the protection of privacy rights in the processing of personal data in their information systems. When privacy rights are violated, the damage can be substantial and sometimes irreparable. Consumers seem to be willing to pay for privacy protection if privacy information is very clearly present on websites or applications (Tsai et al., 2011). On the other hand, it appears that consumers are also inclined to share personal data if they receive some (economic) gain in return (Acquisto et al., 2006). There is a lot to improve when it comes to the effectiveness and efficiency of the of the respect for privacy rights by the Dutch Data Protection Authority. This supervisory body suffer from a structural capacity shortage and the need for a simpler supervisory method is great. However, organizations lack a structured framework of principles, strategies, and tactics to neatly secure privacy in their information systems.

The monitoring of compliance with privacy rights in the processing of personal data is imperfect. Monitoring often takes place in the classic vertical manner, which requires significant capacity that the supervisory body, the Personal Data Authority (AP), do not have. The supervisory body can only act

reactively and have insufficient opportunity to give substance to their function as an authority or advisory body. The hypothesis in this research is that by using a privacy control framework (PCF), compliance monitoring can be more effective and efficient through horizontalization.

It is of great importance for the individual whose personal data is being processed that organizations that process this personal data in their information systems adhere to applicable laws and regulations. This is called compliance. Failure to comply with laws and regulations is called non-compliance. Non-compliance can lead to sanctions by the monitoring authority, varying from a substantial fine or the withdrawal of a license. It can also lead to damage to the organization's reputation. That is why compliance is high on the agenda of many organizations. Compliance is often seen as a means to manage risk rather than an end in itself. The question is therefore not whether but how to prevent non-compliant use of information systems. In any case, it is not achieved by mitigating all possible risks of non-compliance with a laundry list of measures. The study investigated whether privacy could be better ensured by means of a PCF based on privacy by design (PbD). In addition, the study tested whether horizontal monitoring can be applied in relation to compliance and whether this leads to improved and more effective monitoring. Against this background, the study posed the following main question.

RQ: How can a privacy control framework, based on Privacy by Design principles, contribute to the implementation of Horizontal Monitoring?

This paper is structured as follows: Section 2 discusses the methodology of this qualitative research. The results are presented in Section 3, followed by discussion of the research findings in relation to existing literature and interviews in Section 4. In the conclusion, the final findings and possibilities for follow-up research are described.

2. METHODOLOGY

A relatively large amount of scientific literature is available on PbD. With respect to horizontal monitoring, several major studies have been conducted in the tax industry in recent years. However, horizontal monitoring in relation to privacy and the protection of privacy has not been studied quite often in the academic world. The existing theories regarding compliance form the starting point of the research. This means that in this qualitative research, a deductive approach was chosen. Deductive research assumes a top-down approach, in which inferences are made from a general theory to a particular theory. Therefore, a literature review was undertaken as the foundation for the research. The result of the research is an artefact, the PCF, which characterizes the research as design science. In addition to the literature review, data was also collected through semi-structured interviews.

2.1 DESIGN SCIENCE CYCLE

In this research, the design science cycle was used to design the PCF. The design science cycle was designed by Wieringa and described in detail in his 2014 book *Design Science Methodology*. This method finds its origin in Hevner's design science method (Hevner et al., 2004). Design science allows

the researcher not only to explore, describe, or explain a particular phenomenon but also to design or recommend solutions to a particular problem (Dresch et al., 2019). The design science cycle consists of four phases that are completed when designing the artefact. In Figure 1, clockwise, starting at the top right these are problem investigation, treatment design, treatment validation, and treatment implementation.

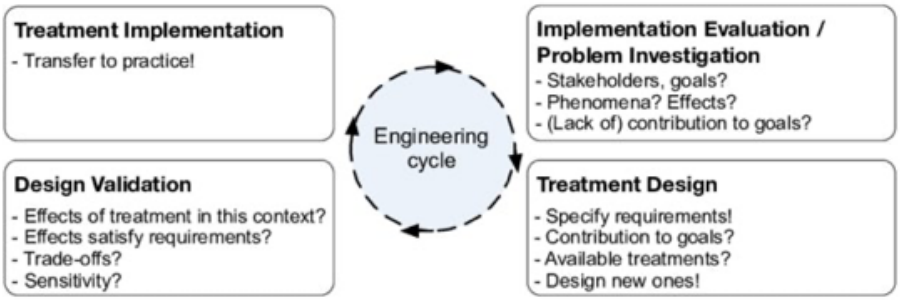

Figure 1, Design science cycle by Wieringa.

Two activities are distinguished: 1) designing an artefact and 2) empirical investigation of the artefact's applicability. The implementation of the artefact (top left of Figure 1) is outside the scope of the research. The problem research phase of this study examines what concepts are already known and applied elsewhere. It examines what takes place in that context, and what causes, and effects are involved. Next, the effect of the PCF is examined in relation to horizontal monitoring. In the solution design phase, the design requirements are specified, and various context variables are considered. It is important for an organization to consider the extent to which the artefact contributes to improved compliance in the processing of personal data and, at the same time, simplifies monitoring for both the organization and supervisory body. It is therefore important that the artefact serve a clear purpose and not merely mitigate recognized compliance risks or lead to needless bureaucracy. Based on literature and data from interviews, among other sources, the draft design is adjusted. In the final phase, the design is validated, and whether the PCF is useful as a solution to the identified problem is considered: “Does the artefact lead to improved compliance and a more effective and efficient monitoring methodology”.

2.2 DATA COLLECTION

With respect to PbD and horizontal surveillance, scholarly and non-scientific articles were selected based on three criteria: time, language, and type. We decided to use only articles written after 2000 in Dutch or English. An exception is the 1890 article by Warren and Brandeis regarding the origin of privacy. An effort was made to only use literature that has been subject to peer review. With respect to horizontal monitoring, this was not possible in all cases. However, the literature used was written by leading scientists with expertise in that field. The literature on horizontal monitoring is limited primarily to professional literature in the tax context. Regarding PbD, a great deal of literature can be found that primarily deals with the interpretation of the principles and their application in the field of system development.

Internet searches yielded 203 articles, from which the 68 most relevant articles were selected. The selected literature was read, studied, and manually analysed. The selection of literature took place according to Liberati's Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) method (Liberati et al., 2009). Figure 2 details the steps. This resulted in a total usable selection of 68 items for the entire study.

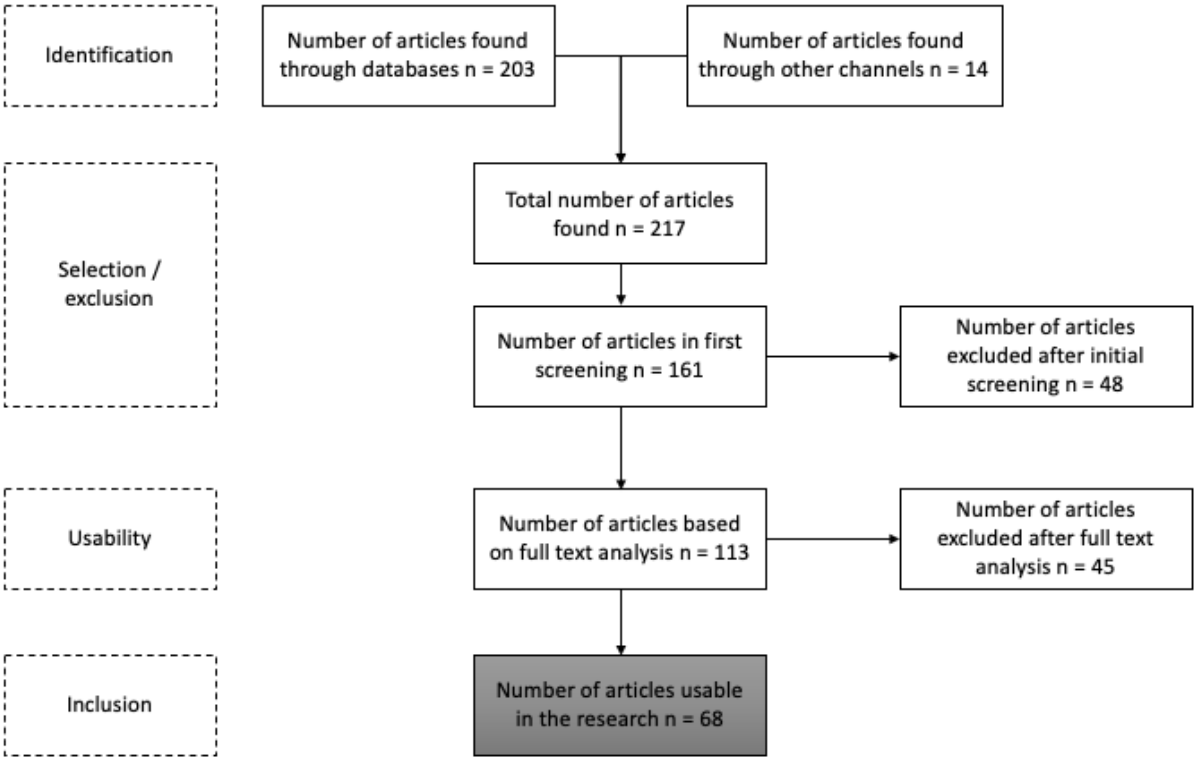

Figure 2, Selection of articles used in the study following Liberati et al.'s method.

Semi-structured interviews were also conducted to outline the context of the study and to test the usefulness of the designed PCF in relation to horizontal monitoring. The interviews were manually processed and analysed by means of an automated tool. The interviews were held with professionals in the organization who work daily with compliance regarding the General Data Protection Regulation (GDPR) and have contact with the supervisory body. The insights of the respondents provide a useful picture of the applicability of the PCF and are discussed in Section 4 of this paper.

2.3 PRIVACY BY DESIGN

Using the seven principles of PbD, a PCF was designed. We examined whether a framework based on PbD principles leads to improved compliance. This coherent set of control measures is also called a PCF (Ridderbeekx & Scheuller, 2018). In implementing a PCF, an organization goes beyond simply meeting the legal requirements of the GDPR; however, in doing so, they can ensure that the oversight to which they are subject is simplified.

In the scientific literature, PbD was not a common term (Lieshout et al., 2012). Cavoukian (Cavoukian, 2009) introduced the term in the 1990s. However, PbD has subsequently evolved into a broader approach (Cavoukian, 2009) that involves not only technical safeguards but also safeguards in business processes and changes in corporate culture. Privacy by design is a fundamental approach that takes privacy into account as early as during the development of information systems (Everson, 2017). Hoepman calls PbD a design philosophy (Hoepman, 2020). The principles of PbD are listed and explained briefly below.

1. Proactive not reactive; preventative not remedial

The PbD approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy-invasive events before they happen. In short, PbD comes before the fact, not after.

2. Privacy as the default

Privacy by design seeks to deliver the maximum degree of privacy by ensuring that personal data is automatically protected in any given IT system or business practice. If an individual does nothing, their privacy remains intact. No action is required on the part of the individual to protect their privacy; it is built into the system by default.

3. Privacy embedded into design

Privacy by design is embedded into the design and architecture of IT systems and business practices. The result is that privacy becomes an essential component of the core functionality being delivered.

4. Full functionality – positive-sum, not zero-sum

Privacy by design seeks to accommodate all legitimate interests and objectives in a positive win-win manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made.

5. End-to-end security – lifecycle protection

Privacy by design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion.

6. Visibility and transparency

Privacy by design strives to provide all interested parties with insight into and transparency about the processing of personal data. People must be possible for individuals as well as for the organization and supervisory bodies.

7. Respect for user privacy

Above all, PbD requires all stakeholders to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options.

Privacy by design is described as a holistic concept that can be applied across a variety of organizational operations, including information technology, business practices, business processes, the physical environment, and networked infrastructure(Cavoukian, Polonetsky, & Wolf, 2010). In addition, PbD is defined in Article 25 of GDPR as 'data protection by design and by default'.[1] Given that PbD as a concept has been broadly embraced and formally embedded in laws and regulations, it was chosen as the guiding principle of this research to shape the PCF.

3. RESULTS

This section describes the results of the study. First, the results regarding horizontal monitoring are described. The emphasis is on the shift from classic vertical to horizontal monitoring. Then, the designed PCF is described, with a focus on the way it was established. Finally, the operation of the framework is explained.

3.1 HORIZONTAL MONITORING

Raaijmakers (Raaijmakers, 2016) writes that supervisory bodies have traditionally struggled with the question of where to place the emphasis of their monitoring policies and how to deploy most effectively their often scarce monitoring capacity. Denkers (Denkers et al., 2013) has conducted research on this and conclude that little is known about the effectiveness of sanctions, control strategies, or enforcement styles on regulatory compliance by organizations. What does emerge is that almost every monitoring relationship has four specific characteristics. These are conflict of interest, unequal information position, inequality of power, and involuntariness.

- *Conflict of interest*: An organization's interests differ from those of the supervisory body. A regulator has been appointed by the government to reinforce and safeguard certain public values. This also includes an advisory function, which the supervisory body should fulfil. This results in tension between the supervisory body and the organization.

- *Unequal information position*: There are unequal information positions, also referred to as information asymmetry. Organizations know what risks manifest internally, but the supervisory body have insight into the monitoring process and how it responds to shortcomings.

- *Power imbalance*: Based on the law, supervisory bodies have instruments to enforce compliance and the power to take punitive action. On the other hand, according to Mendoza et al. (Mendoza & Wielhouwer, 2015) and Van der Hel and Siglé (van der Hel & Siglé, 2019), a supervisory body can also advise.

- *Involvement*: The supervisory body and the supervised did not choose each other but must work with each other. The law gives the supervisory body democratic legitimacy. A positive effect for

[1] See recitals 78 and 108 of the Preamble to Regulation (EU) 2016/679.

organizations is that they can also use monitoring as quality assurance and thus have a learning effect (Raaijmakers, 2016).

Denkers et.al., summarize these characteristics as the ‘inherent unpredictability’ in monitoring relationships. The organization and the supervisory body cannot foresee each other's behaviour. This unpredictability leads to a bureaucratic and hierarchical monitoring relationship. Therefore, methods are sought to make this relationship more predictable and more equal. This explains the emergence of horizontal monitoring.

Since the beginning of this century, the tax authorities have started to use so-called corporate compliance programs (CCP) as part of their overarching compliance risk management strategy. The introduction of horizontal monitoring fits within this development. The principles are understanding, mutual trust, and transparency. It reduces the inherent unpredictability that results from unequal information positions and power imbalances, which are so characteristic of classic vertical monitoring relationships. The aim of horizontal monitoring is to simplify monitoring, bring it forward in the process, and implement it more efficiently. The Stevens Committee (Stevens Committee, 2012) states that if horizontal monitoring works, it will lead to better compliance, lower compliance costs, and stronger cooperation with monitoring authorities. Horizontal monitoring is mainly used in the tax sector between the tax authorities and large organizations. In horizontal monitoring, the course is shifted from full control to risk management. By making a sharp distinction between high-risk and low-risk businesses (more selective monitoring), room is created to deploy control capacity where it is most needed. Horizontal monitoring is characterized by its responsive enforcement style, which means that the supervisory body intervenes where necessary and assumes the responsibilities of the organization where they can. Horizontal monitoring is in line with developments in society, where the individual responsibilities of organizations and governments are transparent but are also enforced (Burgemeestre et al., 2009)

The introduction of horizontal monitoring fits in with a development in which alternative forms of monitoring are sought; the aim of these forms of monitoring is to turn monitoring based on distrust into monitoring based on trust (Huiskers & Gribnau, 2019). Horizontal monitoring has three pillars: mutual trust, understanding, and transparency.

- *Mutual trust* represents the trust that a supervisory body can derive from internal control instruments, such as the PCF. Mutual trust is necessary in a horizontal monitoring relationship to reduce information asymmetry (Burgemeestre et al., 2010 p.8).

- *Understanding* relates to the fact that both parties understand each other's position and sometimes conflicting interests. Huiskers-Stoop (Huiskers-Stoop, 2015) calls understanding each other's needs and aspirations the starting point of the horizontal relationship.

- *Transparency* means openness about the risks and the corresponding measures an organization takes with regard to these risks. Giving substance to the advisory function also fits here.

Horizontal monitoring is therefore aimed at realizing a more equal and cooperative relationship between the organization and the supervisory body in which compliance must be strengthened in ways other than control and the threat of sanctions. According to Raaijmakers (Raaijmakers, 2016), taking the vertical, classical relationship as a starting point, horizontal monitoring is a way of altering the monitoring relationship with the goal of making the relationship more equal. This paradigm shift is illustrated in Figure 3.

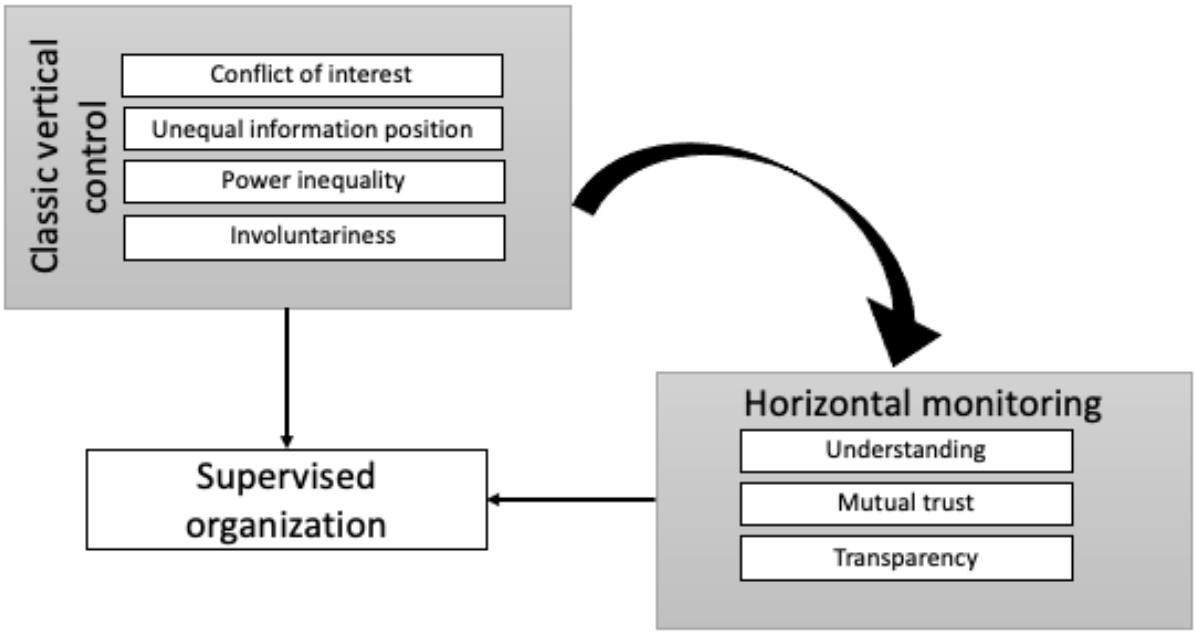

Figure 3, Paradigm shift from vertical to horizontal monitoring.

3.2 DESIGN OF PRIVACY CONTROL FRAMEWORK

Securing privacy requirements and modelling requirements to provide privacy protection has become increasingly important (Guarda & Zannone, 2009). As indicated above, the PbD philosophy was chosen as the starting point for the design of the framework. First, 11 requirements were formulated based on legal requirements from the GDPR and horizontal monitoring to give the PCF a clear objective. Eight of these requirements have their origin in the GDPR and focus on the rights of the individual with respect to the processing of personal data. This selection is also supported by literature from Hoepman (Hoepman, 2014) (Danezis et al., 2015) and Perera (Perera et al., 2016) and the AP's GDPR manual (Schermer et al. 2018 p.73). The other three criteria, understanding, mutual trust and transparency, are defined as requirements because these requirements are used to examine the application of the framework in relation to the usefulness of horizontal monitoring.

One objection to the PbD method, according to Hoela, is that the method is too vague, and the principles are formulated in to abstract a manner (Hoela & Chen, 2016). Therefore, the study translated the vague

PbD principles into a concrete and practical interpretation. Colesky, Hoepman (Colesky et al., 2016) and Perera (Perera et al., 2016) formulate eight strategies to use in an initial translation. These strategies are used in the PCF to take a first step toward concretizing the PbD principles. The eight strategies can be divided into data-oriented strategies and process-oriented strategies. The data-oriented strategies are technical in nature and deal with the processing of the personal data. Next, these strategies must be converted into concrete tactics to give practical substance to each strategy. A total of 25 tactics were selected from the literature. Figure 4 shows which strategies are data oriented, which are process oriented, and the tactics that give practical substance to them.

Data Oriented (technical in nature)			Process Oriented (organizational in nature)		
				Inform	Notify
	Minimize	Select			Warn
		Exclude			Explain
		Destroy		Control	Consent
		Delete			Choice
	Separate	Isolate			Correct
		Distribute			Delete
	Abstract	Group		Enforce	Confirm
		Generalize			Enforce
	Hide	Constraint			Manage
		Encrypt		Demonstrate	Capture
		Dissociation			Audit
		Anonymize			Report

Figure 4, Strategies and tactics to distinguish data-oriented and process-oriented strategies.

3.3 OPERATION OF THE FRAMEWORK

The PCF should be applied in the following way. In Figure 5, the left-hand column contains the requirements derived from the GDPR and horizontal monitoring. The organization may want to pursue one or more of these requirements as an objective. At the top of the PCF, the seven principles of PbD are listed. For each requirement, we determined, based on literature, which principles contribute to the fulfilment of that specific requirement. Subsequently, the organization can see what strategies are available to implement the principles. Hoepman (Hoepman, 2020) (Colesky et al., 2016) and (Danezis et al., 2015) write that strategies ensure that the principles formulated at a high level of abstraction become tangible and give direction to the PCF. It is important to go one level deeper from the strategies and provide practical tactics. In total there are 25 tactics that shape and clarify the strategy (Figure 4). For example, it can be deduced that to concretize the strategy 'abstracting', the tactics 'grouping' and 'generalizing' can be used.

For example, the requirement 'right to object' (R07) comes from the GDPR. In the PCF (Fig. 5), crosses have been made to indicate that principles PbD 6 and PbD 7 fulfil this requirement. For the requirement R07 'objection', it is necessary to apply the strategies inform, verify, and demonstrate (see Fig. 4). A next step is to select the corresponding tactics. In the case of the 'inform' strategy, the tactics 'notify',

'warn', or 'explain' can be chosen to make the strategy tangible. Informing the individual can be done by simply making the privacy policy available on a website or in an app.

PRIVACY CONTROL FRAMEWORK			PbD01 Proactive not reactive	PbD02 Privacy by default	PbD03 Privacy by design	PbD04 Retain full functionality	PbD05 End-to-end security	PbD06 Visible and transparency	PbD07 User central
Requirements AVG									
R01	Right to information	*A data subject must be informed that their personal data is being processed and for what purpose.*			x			X	X
R02	Right of access	*The data subject has the right to know whether an organization processes their personal data and which ones.*						X	X
R03	Right to rectification and addition	*A data subject has the right to have incorrect personal data concerning their rectified.*	X	x					X
R04	Right to erasure	*An organization must delete personal data if it is no longer needed, if the data subject withdraws their consent or if it has been obtained unlawfully.*	X	x		X	x		X
R05	Right to restriction of processing	*The personal data is 'frozen' after processing and may not be further processed or changed.*		x	X		X	X	
R06	Right to portability / data portability	*A data subject has the right to obtain his personal data for transfer.*	X		X		X		X
R07	Right to object	*A data subject has the right to object to the processing of their personal data.*						X	X
R08	Right regarding automated decision-making and profiling	*Organizations should not make decisions about data subjects based solely on automated processing.*			X		X	x	X
Requirements Horizontal Monitoring									
R09	Understanding	*Organizations and regulators understand the context and dynamics of each other's position and sometimes respect conflicting interests.*				x		X	x
R10	Mutual trust	*Organizations and supervisors derive confidence from the operation of the internal control mechanism.*	X		X		X	X	X
R11	Transparency	*Organizations provide openness about the risks and the corresponding measures, and supervisors about parts to be checked.*	X	X	X			X	x

Figure 5, Privacy control framework based on privacy by design principles.

The example of right to object (R07) described above looks schematically as follows. Here the right to object is the starting point, and the organization choose to realize this using PbD principle 6. This principle has three implementation strategies, including 'inform'. To further concretize the strategy 'inform', the tactics 'notify', 'warn', and 'explain' can be used.

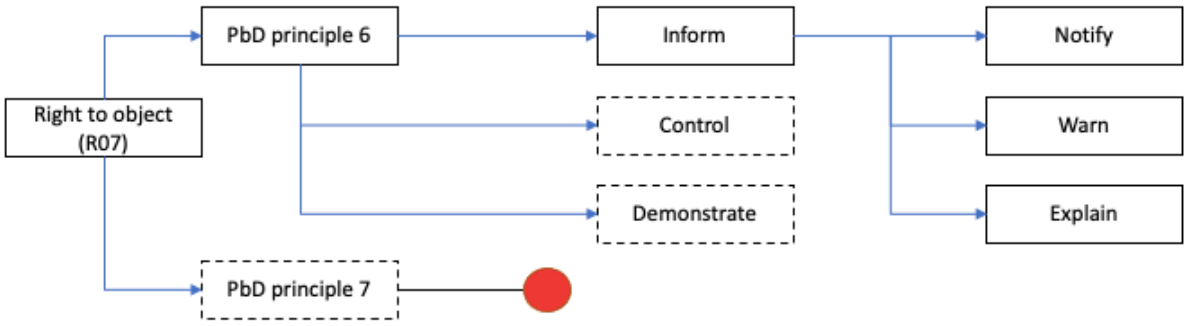

Figure 6, Example of requirement right to object (R07) shown in a flowchart.

4. CONCLUSION AND DISCUSSION

Respect for privacy rights is important in the processing of personal data. However, it appears that guaranteeing these rights is difficult and that monitoring is seriously lacking. The media frequently report on violations of privacy rights or infringement of laws and regulations. In a newspaper article, the chairman of the AP stated in no uncertain terms that there is no monitoring capacity and that the backlogs are 'ridiculous'.[2] This study therefore not only examined whether a PCF promotes the guarantee of privacy rights but also whether it can contribute to simplifying monitoring. For this purpose, the parallel with horizontal monitoring in the tax industry was examined. The reason is that the tax industry lacked the capacity to check tax returns of large organizations, among other entities, and that a more effective and efficient method was sought. At the beginning of this century horizontal monitoring was successfully introduced in that industry and has been used extensively nationally and internationally.

The first conclusion is that the PCF based on the PbD principles helps organizations with compliance regarding the processing of personal data. The requirements from the GDPR give the framework a compliance objective. The principles help to achieve this compliance but require further concretization in the form of strategies and tactics. At that point, the framework becomes practical and operationally deployable.

A second conclusion from the study is that the PCF contributes to the fulfilment of the three criteria of horizontal monitoring: understanding, mutual trust, and transparency. Mutual trust and transparency are enhanced by the framework. In addition, the framework serves as an instrument to facilitate discussions between organizations and the supervisory body, which is important to form mutual trust and transparency. The criteria 'understanding' appears to be unruly. Interviews and literature by Huiskers-Stoop (Huiskers-stoop, 2020) and Gribnau (Huiskers & Gribnau, 2019) among others, show that understanding only arises when parties know each other well, are transparent, and trust each other mutually. Understanding is thus built when trust and transparency are strengthened. In particular, the 2017 survey by the Tax Administration confirms that organizations are more focused on working compliantly when they have a better working relationship with the regulator. That working relationship requires conversations back and forth.

A third conclusion is that horizontal is likely to contribute positively to more efficient and effective, as in the tax industry. This is because horizontal is equivalent and therefore less hierarchical, and more attention is paid to the advisory relationship. This an equal form of monitoring has the positive effect of being less time-consuming. Given the supervisory body's capacity problems, does this help both ways. The supervisory body has more capacity at their disposal for real monitoring and enforcement in the event of abuses and for fulfilling their advisory function from their position as an authority. The organization also benefits from the latter if they turn to the supervisory body with compliance issues.

[2] https://www.trouw.nl/binnenland/voorzitter-autoriteit-persoonsgegevens-de-achterstanden-zijn-zo-groot-dat-het-lachwekkend-is~bb44d7a8/

Horizontal monitoring has some limitations. First, it is important to note that horizontal monitoring must be implemented on a voluntary basis. If an organization or the supervisory body do not see any added value, horizontal monitoring becomes a target, and the effect will be lessened. A second observation is that a horizontal monitoring relationship also requires commitment. Intrinsic motivation is required not only to establish the relationship but also to perpetuate it. In a horizontal monitoring relationship, monitoring can be improved by the supervisory body taking on a more advisory role, for example. This has advantages for both parties if it leads to increased compliance. After all, 'who is opposed to complying with statutory rules'. However, a horizontal monitoring relationship does require an investment of time to hold the essential talks that go with it. Both organizations will have to invest in this.

In addition, horizontal monitoring cannot be considered a panacea; scientists also make critical remarks. The Stevens Committee advises describing clear criteria organizations must meet to qualify for horizontal monitoring. To date, there are no such criteria. Huiskers-Stoop (Huiskers-Stoop, 2015) is critical about normatively determining the effectiveness of horizontal monitoring, a criticism that is also given from the political angle. Huiskers-Stoop highlights in her research that it is necessary to be able to test objectively why HM can be agreed upon with one organization and not another. When is an organization good enough, and can it lose this qualification?

Finally, De Widt's 2017 study (De Widt, 2017) comments on the admission to horizontal monitoring and makes several recommendations in his research. De Widt writes, 'This high level of interaction will especially occur during the initial stage of cooperative compliance, when a relatively large number of businesses are likely to need more feedback to improve their level of control.' The report therefore advises that organizations should not be admitted to horizontal monitoring until sufficient knowledge and expertise is available within the organization, for example, to set up a PCF.

This answers the main question of the study: What does a PCF based on PbD principles for the implementation of horizontal monitoring look like? Above all, it must have a concrete application and make vaguely formulated principles tangible. It must help to improve the dialogue between the supervisory body and organizations to work on mutual trust, understanding, and transparency. In this way, a horizontal monitoring relationship can be established if desired by both parties.

4.1 LIMITATIONS AND FOLLOW-UP RESEARCH

This research also had some limitations. First, it proved impossible to gain access to the supervisory body's office to look at the possibility of horizontal monitoring from their perspective in the context of processing personal data. It would have been helpful to explore how the supervisory body would have seen the supposed improvement in efficiency and effectiveness, and whether a privacy control framework is the right instrument to realize these improvements in terms of content, there was the limitation that horizontal monitoring proved to be less well known outside the tax context than previously estimated. Horizontal monitoring is known particularly in the tax industry and, as such, has been studied from multiple perspectives. Outside the tax context, horizontal monitoring is relatively unknown.

Follow-up research can be conducted to determine whether a horizontal monitoring relationship can be used e.g., in the context of privacy or elsewhere.

Acquisto, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. *ICIS 2006 Proceedings - Twenty Seventh International Conference on Information Systems*, 1563–1580.

Alan R. Hevner, Salvatore T. March, Jinsoo Park, & Sudha Ram. (2004). Design Science in Information Systems Research. *MIS Quarterly*, *28*(1), 75–105. https://doi.org/10.2307/25148625

Burgemeestre, B., Hulstijn, J., & Tan, Y. H. (2009). Towards an architecture for self-regulating agents: A case study in international trade. *CEUR Workshop Proceedings*, *494*, 84–89.

Burgemeestre, B., Hulstijn, J., & Tan, Y. H. (2010). The role of trust in government control of businesses. *23rd Bled EConference ETrust: Implications for the Individual, Enterprises and Society - Proceedings*, 301–313.

Cavoukian, A., & others. (2009). Privacy by design: The 7 foundational principles. *Information and Privacy Commissioner of Ontario, Canada*. Retrieved from https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

Cavoukian, A., Polonetsky, J., & Wolf, C. (2010). SmartPrivacy for the Smart Grid: embedding privacy into the design of electricity conservation. *Identity in the Information Society*, *3*(2), 275–294. https://doi.org/10.1007/s12394-010-0046-y

Colesky, M., Hoepman, J. H., & Hillen, C. (2016). A Critical Analysis of Privacy Design Strategies. *Proceedings - 2016 IEEE Symposium on Security and Privacy Workshops, SPW 2016*, 33–40. https://doi.org/10.1109/SPW.2016.23

Commissie Stevens. (2012). *Fiscaal toezicht op maat*. 1–128.

Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.-H., Metayer, D. Le, Tirtea, R., & Schiffner, S. (2015). Privacy and Data Protection by Design - from policy to engineering. In *European Cyber Security Perspectives*. https://doi.org/10.2824/38623

de Widt, D. (2017). Dutch Horizontal monitoring. The Handicap of a Head Start. *FairTax Working Paper Series*, *13*(September 2017), 1–39.

Denkers, A. J. M., Peeters, M. P., & Huisman, W. (2013). *Waarom organisaties de regels naleven*.

Dresch, A., Pacheco Lacerda, D., & Cauchick-Miguel, P. A. (2019). Design science in operations management: conceptual foundations and literature analysis. *Brazilian Journal of Operations & Production Management*, *16*(2), 333–346. https://doi.org/10.14488/bjopm.2019.v16.n2.a13

Everson, E. (2017). Privacy by design: Taking ctrl of big data. *Cleveland State Law Review*, *65*(1), 27–43.

Guarda, P., & Zannone, N. (2009). Towards the development of privacy-aware systems. *Information and Software Technology*, *51*(2), 337–350. https://doi.org/10.1016/j.infsof.2008.04.004

Hoela, T., & Chen, W. (2016). The principle of data protection by design and default as a lever for bringing pedagogy into the discourse on learning analytics. *ICCE 2016 - 24th International Conference on Computers in Education: Think Global Act Local - Workshop Proceedings*, 113–121.

Hoepman, J.-H. (2014). Privacy Design Strategies (extended abstract). *SEC 2014: ICT System Security and Privacy Protection*, *428*(10532), 446–459.

Hoepman, J. (2020). *Privacyontwerpstrategieën (Het Blauwe Boekje)*.

Huiskers-Stoop, E. (2015). *De effectiviteit van horizontaal belastingtoezicht*.

Huiskers-stoop, P. R. R. E. N. E. A. M. (2020). *De doorontwikkeling van horizontaal belastingtoezicht*. (9), 368–382.

Huiskers, E., & Gribnau, J. (2019). Cooperative Compliance and the Dutch Horizontal Monitoring Model. *Journal of Tax Administration*, *5*(1), 66–110.

Liberati, A., Altman, D. G., Tetzlaff, J., Mulrow, C., Gøtzsche, P. C., Ioannidis, J. P. A., … Moher, D. (2009). The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: explanation and elaboration. In *Journal of clinical epidemiology* (Vol. 62). https://doi.org/10.1016/j.jclinepi.2009.06.006

Lieshout, M. Van, Kool, L., Bodea, G., Schlechter, J., Schoonhoven, B. Van, & Kennisopbouw, I. (2012). *Stimulerende en remmende factoren van Privacy by Design in Nederland*.

Mendoza, J. P., & Wielhouwer, J. L. (2015). Only the carrot, not the stick: Incorporating trust into the enforcement of regulation. *PLoS ONE*, *10*(2), 1–18. https://doi.org/10.1371/journal.pone.0117212

Perera, C., McCormick, C., Bandara, A. K., Price, B. A., & Nuseibeh, B. (2016). Privacy-by-design framework for assessing internet of things applications and platforms. *ACM International Conference Proceeding Series*, *07-09-Nove*, 83–92. https://doi.org/10.1145/2991561.2991566

Raaijmakers, K. (2016). Inherente onvoorspelbaarheid in toezichtrelaties. *Jaarboek Compliance 2016*, 65–79.

Ridderbeekx, E., Scheuller, S., Ridderbeekx, W. E., & Scheuller, S. (2018). *Een nieuw Privacy Control Framework als onderdeel van de informatiehuishouding*. (september), 1–16.

Schermer, B. W., Hagenauw, D., & Falot, N. (2018). *Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming*. 98. Retrieved from https://www.rijksoverheid.nl/documenten/rapporten/2018/01/22/handleiding-algemene-verordening-gegevensbescherming%0Ahttps://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/handleidingalgemeneverordeninggegevensbescherming.pdf

Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research*, *22*(2), 254–268. https://doi.org/10.1287/isre.1090.0260

van der Hel, L., & Siglé, M. (2019). Herijking horizontaal toezicht: noodzakelijk kwaad of logisch gevolg? *Tijdschrift Voor Toezicht*, *10*(1), 13–25. https://doi.org/10.5553/tvt/187987052019010001004