

The Carrot, the Stick and the Hand that wields them:
Regulation of Privacy in the Netherlands
An Analysis of the Enforcement of Dutch Privacy Law



Student: Eberly Haalboom

Student number: 9926658

Supervised by: Dr. J. Matthys

Leiden University – Faculty of Governance and Global Affairs

MSc Public Administration – track Crisis and Security Management

Date: 21st of March 2018

Index

1 Introduction	4
1.1 The regulation of privacy in the Netherlands	4
1.2 Research question	6
1.3 Societal and scientific relevance	6
1.4 Thesis outline	7
2 Theoretical framework	8
2.1 Concepts of privacy regulation	8
2.1.1 Privacy	8
2.1.2 Regulation and enforcement	9
2.2 Theory and literature on enforcement	11
2.2.1 The regulatory process.....	11
2.2.2 Enforcement.....	12
2.2.3 Responsive regulation.....	14
2.2.4 Impact on the regulatory process	16
2.3 Overview	17
3 Methodology	18
3.1 Research design	18
3.2 Justification	19
3.3 Data gathering	21
3.4 Operationalization	22
3.4.1 Currently deployed instruments.....	25
3.4.2 Organisational resources.....	25
3.4.3 Enforcement instruments	26
3.4.4 Level of discretion	26
3.4.5 Applicable law	27
3.5 Validity and reliability	27
4 Analysis	29
4.1 The applicable law and the Dutch DPA	29
4.2 Testing the propositions	32
4.2.1 Currently deployed instruments.....	32
4.2.2 Organisational resources.....	37

4.2.3 Enforcement instruments	41
4.2.4 Level of discretion	44
4.2.5 Applicable law	48
4.3 Results: likelihood of the propositions	51
5 Conclusion	52
5.1 Summary of analysis outcome	52
5.2 Reflection on results.....	53
Abbreviations	55
References.....	56

1 Introduction

1.1 The regulation of privacy in the Netherlands

In the current information age the fast paced evolution of information technology is one of the drivers of globalization and an enabler of processing ever-growing volumes of personal data by many actors in society. Therefore privacy protection is more essential than ever before (Davidson, Hordern, Jackson, Lee, Levin, Pastor, Patrikios, Room, Sugard & Taranto, 2012, p. 3). According to a study, since the end of 2011, more than eighty countries have data protection regimes. However, restrictions related to the processing of personal information and the enforcement of privacy laws vary greatly on a national level (Swire & Ahmad, 2012, p. 30).

The Netherlands, being a member state of the European Union (EU), adheres to European privacy law on which its national privacy law, the Dutch Data Protection Act (*Wet bescherming persoonsgegevens* [Wbp]), is based. To enforce Dutch privacy law the Dutch Data Protection Authority (DPA), in Dutch called *Autoriteit Persoonsgegevens*, is an independent governmental organisation tasked with the investigation of suspected infringements and authorized to deploy a range of instruments once non-compliance to privacy law has been ascertained. The instruments the Dutch DPA can use to enforce compliance varies from persuasive forms of communication to the more coercive –or punitive – authority to impose fines up to ten per cent of an organisation's annual revenue, introduced on the 1st of January 2016 (Autoriteit Persoonsgegevens [AP], *Boetebeleidsregels*, 2016, p. 3). On the same date, the obligation for organisations to report data leakages regarding personal information to the Dutch DPA came into effect (AP, *De meldplicht datalekken in de Wbp*, 2015, p. 8).

The European General Data Protection Regulation (GDPR) formally entered into force on the 25th of May 2016, but will be applicable –and enforced– on the 25th of May 2018 replacing national privacy legislation within the EU. The EU has created a time window of two years to adapt to the GDPR and it is generally understood this preparation time is needed due to some onerous obligations under the GDPR (Allen & Overy, *The EU General Data Protection Regulation 2017*, p. 2-9).

In the light of the previously mentioned societal and legislative developments regarding privacy regulation in the Netherlands, it is interesting to zoom in on the enforcement efforts by the Dutch DPA.

	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016
<i>Official investigation</i>	11	73	70	80	83	49	95	108	60	85	58	73	85	43	197
<i>Fine (obligation to report processing)</i>	0	1	35	9	3	0	0	0	0	0	0	0	0	0	-
<i>Order subject to non-compliance penalty</i>	0	1	5	2	0	39	68	26	35	6	12	19	13	17	20
<i>Cease and desist order</i>	1	1	1	1	2	0	-	-	-	-	-	-	-	-	-
<i>Objection</i>	1	2	8	15	2	5	5	6	10	6	7	6	11	15	15
<i>Appeal</i>	1	2	4	15	2	9	2	2	10	3	8	3	7	1	7

Figure 1. *Coercive instruments of the Dutch DPA (Jansen, 2017, Gegevens uit jaarverslagen, para. 2)*

Figure 1 shows the relevant numbers regarding the Dutch DPA's use of its more coercive enforcement instruments, based on the Dutch DPA's annual reports of the years 2002 through 2016. Since 2008, the numbers regarding orders subject to non-compliance penalty and cease and desist orders have been merged in the annual reports of the Dutch DPA, from then on only reflecting orders subject to non-compliance penalty. The fine due to violating the obligation to report the processing of personal information has not been issued by the Dutch DPA since 2007 and has been removed from the legislation since January 2016. The GDPR does no longer encompass the obligation to report the processing of personal information (not be confused with the obligation to report data leakages regarding personal information). The numbers in figure 1 show a relatively low level of coercion in the enforcement of Dutch privacy law by the Dutch DPA.

The relevant numbers of the annual report of 2016, published by the Dutch DPA in May 2017, have been added to the table in figure 1 by the author. The increase in official investigations is the result of the, in 2016 introduced, obligation to report data leakages regarding personal information (AP, *Bijlage jaarverslag 2016*, p. 5). In more detail, the Dutch DPA reports that in 2016 there have been 5500 reports of data leakages regarding personal information of which 4000 have been initially investigated, leading to 100 official warnings and dozens of cases under further investigation by the Dutch DPA (AP, *1 jaar meldplicht datalekken: facts & figures 2016*). The numbers show that the increase in official investigations did not result in a significant increase of cease and desist fines or objections and appeals to enforcement decisions by the Dutch DPA. Furthermore, the since the 1st of January 2016 intensified arsenal of –directly impossible– fines has not been used once (AP, *Bijlage jaarverslag 2016*). These numbers are supported by a quick scan of media reports regarding acts of enforcement by the Dutch DPA from the beginning of 2015 to the

end of 2016, which does not show a significant increase in severity, or number, of more coercive enforcement cases.

Looking at the above, it can be stated that even though Dutch privacy law –under the influence of European law– has become more restrictive and the instruments for enforcement have intensified, the cases where the Dutch DPA uses its enhanced tools seem absent. One would expect that the increased volumes of personal data processed by a growing number of actors in –a globalizing– society in combination with the expanded authority and toolkit of the Dutch DPA would lead to an increase in the number of cases where the more coercive enforcement instruments are being applied. The aforementioned developments can be identified as a paradox, which needs to be researched.

1.2 Research question

Taking the paradox as stated in paragraph 1.1 in consideration, the following central research question is formulated:

What factors determine the low level of coercion in the enforcement of Dutch privacy law by the Dutch Data Protection Authority during the period of 2015 through 2016?

1.3 Societal and scientific relevance

From a societal perspective, enforcement of laws is crucial for any society. Without enforcement, laws will become meaningless and governments will lose their legitimacy. Which in worst-case scenarios will lead to failed states. Enforcement of privacy law is essential to societies governed by democratic nation states based on constitutional law –constitutional states– in particular, due to the fact that privacy laws concern the protection of fundamental rights of citizens. Not only against infringements by other citizens or private –commercial– organisations, but also against abuse by the state, or government, itself. Ergo, the fundamental human right of privacy protection is essential to the adequate functioning of constitutional states.

Scientifically, researching the aforementioned paradox can lead to more insight into theories regarding the enforcement of laws, the effectiveness of policies and the dynamics regarding the implementation of supranational policies on a national level. In this specific case, the effectiveness of European policy implementation is researched and relatively close after the United Kingdom has voted to leave the European Union (Brexit) it can be said that the outcome of the European project is not

as predictable as some of the literature might suggest. In that light, theories on European integration will face a period of revisiting and falsification possibly leading to a wider knowledge gap than before.

1.4 Thesis outline

In the following chapter the theoretical framework, which will be used to answer the research question, is discussed. In chapter 3, the methodology and operationalization of the theoretical framework is addressed. After the analysis in chapter 4, the research question will be answered during the conclusion in chapter 5.

2 Theoretical framework

2.1 Concepts of privacy regulation

Before elaborating on the theory and literature, this paragraph addresses the concepts regarding privacy regulation, which are relevant to comprehend in order to answer the research question.

2.1.1 Privacy

Privacy is most commonly defined as an individual's right to be left alone, as well as, the individual's desire to freely choose his or her attitude and behaviour to others.

Privacy is used as a means to protect the individual's independence, dignity and integrity (Swire & Ahmad, 2012, p. 1).

There are four interrelating dimensions, or classes, of privacy: information privacy, bodily privacy, territorial privacy and communications privacy. Bodily- and territorial privacy concerns, respectively, limiting the ability to invade an individual's physical being and limiting the ability to intrude into another individual's environment. Communications privacy entails the protection of all forms of correspondence, i.e. physical- and digital correspondence next to communicative behaviour and apparatus. Information privacy focuses on the establishment of rules to govern the collection and handling of personal information (Swire & Ahmad, 2012, p. 2).

The latter privacy dimension is the most relevant for this research and it introduces the concept of personal information, which can be described as any and all data or information that relates to an identified or identifiable individual. The definition of personal information may vary per jurisdictions across the globe based on the nuance of what is identifiable. As soon as data or information is de-identified, or anonymized, it is nonpersonal information and privacy laws are not applicable. Personal information knows a subset called sensitive personal information, which in most jurisdictions refers to health information. In addition, information regarding an individual's sex life, trade union membership, religious beliefs, political opinion, racial or ethnic origin, finances and social security numbers are often categorized as sensitive personal information (Swire & Ahmad, 2012, p. 4-7).

The processing of personal information is defined as almost anything one may do with personal information: collection, recording, organisation, storage, updating, modification, retrieval, consultation, use, disclosure by transmission, dissemination or

making available in any form, linking, alignment, combination, blocking, erasure and destruction. The processing of personal information knows three kinds of actors. First is the data subject, which is the individual about whom information is being processed. Second is the data controller, which is an individual or organisation that has the authority to make decisions on how and why the personal information is processed and therefore is the focus of most of the obligations under privacy law. Third is the data processor, which is an individual or organisation that processes personal information on behalf of a data controller often in outsourcing constructions that can stretch like chains. Data processors are not allowed to process personal information in such a way that it is out of scope of what the respective data controller is permitted to do with that personal information itself (Swire & Ahmad, 2012, p. 8).

2.1.2 Regulation and enforcement

As stated in the introduction, in the majority –if not all– democratic nation states based on constitutional law, fundamental privacy rights are the subject of regulation.

Regulation can be understood in different ways, not being straightjacketed in one definition. Regulation can be defined as ‘sustained and focussed control exercised by a public agency over activities that are valued by a community’. Alternatively, regulation can be defined as the application of a specific set of commands, or a binding set of rules, by a body devoted to this purpose. In a broader sense, regulation can be defined as all state actions that are designed to influence business or social behaviour. Additionally, regulation can be defined as all forms of social or economic influence affecting behaviour, whether the regulating mechanisms are state based or from other sources in society. This leads to the notion that, next to state institutions, regulators can also be corporations, self-regulators, professional or trade bodies, voluntary organisations and non-governmental organisations. To conclude on the concept of regulation, it should be mentioned that next to restricting behaviour or preventing the occurrence of unwanted activity, regulation can also have an enabling or facilitative character to allow otherwise unlikely outcomes to come into existence (Baldwin et al., 2012, p. 2-3).

Often the motives, or justifications, for regulation are the result of market failure where for different reasons the –uncontrolled– marketplace will not produce behaviour or results in accordance with the public interest. Next to market failure, rights-based and social rationales are adopted to justify regulation. An important

factor to consider here is that to protect human rights, or to further social solidarity, the preferences of market players or other actors in society may be overruled and a paternalistic approach deliberately adopted. In extremis this will lead to the perseverance of regulation while accepting the absence of support of the involved, and fully informed, citizens. In reality the decision to regulate is often based on a combination of the previously described rationales, next to the fact that regulatory strategies themselves have strengths and weaknesses, regarding their design and implementation. This results in the notion that the choice to regulate will have to consist of considering all varieties of solutions, including all their likely deficiencies and side effects, if valid comparisons are to be made (Baldwin et al., 2012, p. 15-23).

This general discussion of the concept of regulation will be concluded with a brief discussion of regulatory failure and, more specifically, enforcement failings. What constitutes a regulatory failure is the subject of debate and depends on different understandings regarding objectives and problem definitions. Regulatory failure usually consists of identifying failings involving poor performance of the core tasks of regulation leading to negative outcomes. One of the core tasks of regulation, which will be discussed in more detail in the following paragraph, is enforcement.

Enforcement can be defined as “the states actions to detect violations, to stop them and to prevent further violation from occurring in the future” (Van Rooij, 2006, p. 227). The primary objective of enforcement is compliance and effective enforcement is seen as the key element to successful implementation of legislation (Kluin, 2014, p. 51). The procedure of regulation and enforcement can be seen as a regulatory regime, which entails an institutional structure and the assignment of responsibilities for performing regulatory actions. The institutional structure is made up of rules prescribing expected behaviour and outcomes, standards that are benchmarks used to measure compliance, mechanisms to determine the degree of regulatory compliance and sanctions for failure to comply with the rules (May, 2007, p. 9). The definition of enforcement used in this research is derived from the DREAM framework, described in more detail in §2.2.1, where enforcement is defined as the application of policies, rules and tools on the ground by a regulator (Baldwin et al., 2012, p. 227-258).

A common manifestation of enforcement failings may be ‘creative compliance’, which consists of the sidestepping of rules and negating regulations without formally breaking them by regulatees. This may lead to the –undesired– displacement, or shift, of risks from a regulated to an unregulated operation. More important in this context

is the generic problem of ‘failure to maintain reputation’ by regulators, which resides at the heart of enforcement failings. If the perception arises that regulators lack the capacity to effectively act against errant operators then politicians, regulatees and other actors will no longer defer to them undermining their legitimacy. In worst case scenarios this could have reputational spill over effects leading to a lack of trust in entire regulatory systems or domains. Without going into too much detail, this paragraph can be concluded to state that in remedying regulatory failure the emphasis should be on relying on redundancy –instead of being dependent of one single instrument or even organisation to realise the desired outcomes– and to allow for contestability in order to prevent closed views or restricted perspectives on failings and the benevolence of particular regulatory instruments (Baldwin et al., 2012, p. 68-82).

2.2 Theory and literature on enforcement

The theoretical framework sets out to clarify enforcement as an element of the broader theoretical concept of regulation. From the theoretical framework a set of propositions will be derived, which will be used to answer the research question.

2.2.1 The regulatory process

In *Understanding Regulation: Theory, Strategy, and Practice* (2012), Baldwin, Cave & Lodge describe regulatory core tasks using the DREAM framework. The acronym reflects the tasks of detecting, responding, enforcing, assessing and modifying, within a sequenced and cyclic regulatory process, which is able to adapt for the challenges regulators encounter seeking to apply enforcement on the ground. The task of detecting aims at gaining information on undesirable and non-compliant behaviour. After a problem has been discovered, the task of responding aims at developing policies, rules and tools to deal with it. By the task of enforcing, the regulator applies the policies, rules and tools on the ground. The task of assessing measures the success or failure in enforcement activities after which the task of modifying adjusts tools and strategies in order to improve compliance and to address problematic behaviour (p. 227).

Although all tasks in the DREAM framework are relevant for continuous adequate regulation, the emphasis for this research is on enforcement, which will therefore be elaborated on in the following paragraph.

2.2.2 Enforcement

There are two distinct approaches regarding enforcement within a range of informal to formal techniques regulators can adopt to gain compliance with the law:

‘compliance’ approaches and ‘deterrence’ approaches. For example, advice, education, persuasion and negotiation are part of the compliance approaches, which range from the subcategories of persuasive, more accommodating, approaches to more insistent approaches. Deterrence approaches, on the other hand, consist of sanctions, or penalties, and prosecutions to deter future non-compliance to the law. Depending on the situation, compliance and deterrence approaches are known to have specific strengths and weaknesses and it is therefore understood not to rely too much on one of the approaches. Instead, establishing a synergy between persuasion and punishment will lead to successful regulation and enforcement should therefore be seen as a progression through different compliance seeking strategies and sanctions (Baldwin et al., 2012, p. 238-243).

In addition to the methods of intervention described above, regulators can intervene at different stages during the processes –i.e. economic or social activity– that lead to harms. Action taken to prevent a dangerous act or situation arising, action taken in response to the act of creating a dangerous situation and action prompted by the realization of a harm can be categorized as, respectively, preventative actions, act-based interventions and harm-based interventions. As with compliance and deterrence approaches there are strengths and weaknesses given the situation in which a certain form of intervention is applied and deploying a mixture of targeted strategies is most likely to secure the desired results on the ground (Ayres & Braithwaite, 1992, p.25; Baldwin et al., 2012, p. 243-246).

As enforcement is a means to achieve a certain level of compliance or elimination of a risk, it is good to understand that enforcement costs have the tendency to escalate as the desired levels of compliance are raised. Referred to by some authors as the problem of the last ten per cent, there is a point at which the costs of further enforcement are no longer justified by the gains. The costs of enforcement consist of the costs of agency monitoring, the expenses of processing and prosecuting cases, the defence costs of accused parties, and the costs of misapplications of law, convicting the innocent and deterring desirable behaviour. The gains from enforcement can be found in the reduction of harmful behaviour by preventing the particular offender from causing harm and by deterring others from doing so. An additional gain is the

reduction of private enforcement costs, due to the fact that prevention of harm by public enforcement agencies saves private actors from having to spend money on protecting their rights. Elaborating on costs and gains regarding enforcement suggest that economic and rational calculations –by regulators and regulatees– are a strong underlying driver of enforcement decisions, which is not always the case. Policy and equitable considerations may often drive enforcement decisions and, as in most scientific discourse, the assumptions of economically rational man may be questioned. In reality, most harms are not the result of rational cost and benefit calculations but the product of human failure, poor information and training, fatigue, short cuts and accidents (Makkai & Braithwaite, 1993, p. 271-291; Baldwin et al., 2012, p. 247-248).

Most of regulation concerns control of, and thus enforcement aimed at, corporations or organisations. This specific group of regulatees know particular issues when it comes to sanctions, the ascertainment of the extent of –criminal– fault and difficulties of proving liability. Organisations may treat sanctions in the form of fines as a business expense and –indirectly– transfer them to customers, or clients, and even employees. Large fines could threaten an organisations existence and as such punish innocent parties like its employees (availability of jobs) and customers (availability of goods and services). A fine could remove cash from an organisation which otherwise could have been used to remedy the issue at hand. Fines that are borne by the organisation may not influence or deter the decision-maker within the organisation and fines do not ensure that the actual problem is remedied or that the cause of failure within the organisation is identified. Alternatives to improve on the described deficiencies of fines are equity fines, punitive injunctions, community service and compensations orders and adverse publicity orders. Hence, once more it is to be mentioned that the described sanctions all have their strengths and weaknesses given the specific situation. Therefore regulators and courts are best off approaching corporate, or organisational, failure with the full array of sanctions within their contemplation. In addition, sanctions should be applied by regulators and courts keeping in mind not only the need to punish and rehabilitate organisations but also the interest of the public in compensation and in more effective compliance (Baldwin et al., 2012, p. 249-254).

2.2.3 Responsive regulation

Moving the regulatory enforcement debate away from the apparent dichotomy between compliance and deterrence, the model of ‘responsive regulation’ is introduced. Responsive regulation entails the concept of the enforcement pyramid, along which the regulator can escalate or de-escalate its response depending on the reaction of the regulatee. The enforcement pyramid consists of layers of response, starting at the base with ‘persuasion’, followed by a second layer ‘warning letter’, continuing in severity or coerciveness to ‘administrative notice’, subsequently followed by ‘civil penalty’, ‘criminal penalty’, ‘license suspension’ and ‘license revocation’ (See figure 2, §2.3). Regulators are presumed to have the preference to initially use less interventionist measures and escalate their response up the enforcement pyramid allowing for regulatory responsiveness. Compliance is most likely when a regulatory agency operates an explicit enforcement pyramid (Ayres & Braithwaite, 1992, p. 25 & 35; Baldwin et al., 2012, p. 259-260; Gunningham & Sinclair, 2017, p. 133-148).

Although responsive regulation remains hugely influential worldwide, many governments and regulators apply it and it has been elaborated on in empirical work, it is also subjected to criticism and reservations.

The first criticism is that in circumstances where, for example, potentially catastrophic risks are being controlled it might not be appropriate to escalate up from the lowest layers of the pyramid but directly resort to its higher levels.

Second, under certain conditions it might be necessary, post-escalation, to move the response down the pyramid, decreasing the punitive character of the approach. This could be the case in a situation where a regulatee has become more inclined to offer greater levels of compliance than before. But moving down the pyramid may not always be easy because the use of more punitive sanctions may prejudice the relationship between regulator and regulatee which is the foundation for less punitive strategies (Ayres & Braithwaite, 1992, p. 19-53).

Third, it may be wasteful to apply the wrong medicine to the patient due to unfamiliarity with the patient. There are certain situations where it is more efficient to first analyse the type of regulatees in order to adapt the regulatory response accordingly. The behaviour of, and thus the response of, regulatees might be more influenced by, for example, the dominant culture in their sector or forces of competition involved. This could make regulatees insusceptible to the initially

deployed level of the enforcement pyramid, which in cases where the regulator is unaware of the regulatees' insusceptibility leads to a waste of enforcement resources.

Fourth, complex enforcement situations where multiple regulators are involved can lead to poor communication –confusion and interference regarding messages and expectations– between regulators and regulatees. This can have a negative effect on any responsive approach to sanctioning, undermining the responsive regulation strategy.

Fifth, the degree of cooperation forthcoming from the regulatee is not the only factor influencing whether a responsive approach is optimal. Many other factors could result in situations where regulators do not choose to escalate through the layers of an enforcement pyramid. Examples are the regulator's level of resources, the size of the regulated population, the kinds of standards to comply to, the observability of non-compliance, the costs of compliance, the availability of financial assistance and the penalty structure. Due to their own organisational resources, cultures, practices and constraints of the broader institutional environment, regulators may be strongly bound to certain compliance strategies. Next to a lack of resources preventing a more punitive approach, regulators could fear political consequences of progression and perceive a lack of judicial, public, or political support. Regulators can be reluctant to trigger adverse business reactions to deterrence strategies and they may find it difficult to assess the need for escalation due to a lack of information about the regulatees' response to existing controls. When a regulator feels the evidence for the highest levels of response is insufficient, it may also be hesitant to escalate. On the other side, regulators can be prone to adopt a more punitive stance regardless of the regulatees' level of cooperativeness. It could be, due to political or media pressure or as a decoy strategy to hide weaknesses elsewhere, that the top of a regulatory organisation has decided to shift to more deterrence or a more punitive style across the board regarding particular regulatees.

Sixth, regulators can be bound to certain strategies forced by legislation, undermining the principle of a wide range of credible sanctions to be available for responsive regulation to work. Legislators can also have failed to provide regulators with sanctions and investigative tools to allow for a progression up the enforcement pyramid. As a result, the proverbial stick can be too small or even non-existent, depriving regulators of an essential tool especially when dealing with more calculating offenders (Ayres & Braithwaite, 1992, p. 19-53). At the other extreme, it

is possible that the stick is so big –and the consequences of using it so grave– that a regulator can simply never use it.

Seventh, an inherent danger of responsive regulation systems is that they involve high levels of discretion and have the tendency to operate in a non-transparent manner. Additionally, this may raise issues of consistency of treatment across different regulatees. Remediating this by generating rules and guidelines could straightjacket responsive regulation within costly bureaucratic controls and the generated rules and guidelines themselves are likely to be under-exposed to democratic control. It is argued that discretionary regimes characterized by close relationships between regulators and regulatees are susceptible to regulatory capture. As a counterbalance public interest groups can be added as a third party to the interaction between regulator and regulatee, introducing its own dilemma's regarding the allocation of power, representation, trust and cooperation within the regulatory process (Ayres & Braithwaite, 1992, p. 54-100; Mendeloff, 1993, p. 719).

The eighth and last criticism would break away completely from responsive regulation and the enforcement pyramid by focussing on measures that lead to designing out potential mischiefs in advance, the screening of regulatees before they endeavour on regulated activities, the restructuring of the relevant industry, relying on non-state controls instead of state sanctioning or emphasizing on systemic sector-wide problems beyond individual non-compliers. In general, it is argued that responsive regulation does not provide the complete answer for designing and applying the instruments in the enforcement toolkit (Baldwin et al., 2012, p. 260-265).

2.2.4 Impact on the regulatory process

Returning to the DREAM framework, it can be stated that a predominant emphasis on increasing the effectiveness of certain tools in order to achieve better enforcement can be tricky. Enforcement can lead to the success or failure of regulation, not only by its influence on the achievement of the right objectives but also by its impact on the quality of the regulatory process. Above all, enforcement should be understood as an activity demanding highly complex trade-offs and balances to be carried out involving issues regarding accountability, due process and expertise. Examples are: punishing infringers versus maximizing compliance levels; preventing creative compliance versus producing easily understood rules; and upholding high levels of discretion to allow for flexible and targeted enforcement versus accountability and fairness. In the

end, enforcement is about making highly complex trade-offs and balances in a way that is justified and, as is emphasized, the need for legitimacy runs through the entire regulatory process (Baldwin et al., 2012, p. 257-258).

2.3 Overview

The theoretical model used for this research is visualized in figure 2. It depicts enforcement as part of the DREAM framework, while expressing it as an enforcement pyramid consisting of different layers increasing in coercive –or punitive– character towards the top. A regulator should be able to escalate through the different layers of an explicit enforcement pyramid depending on the regulatees’ response in order to achieve compliance.

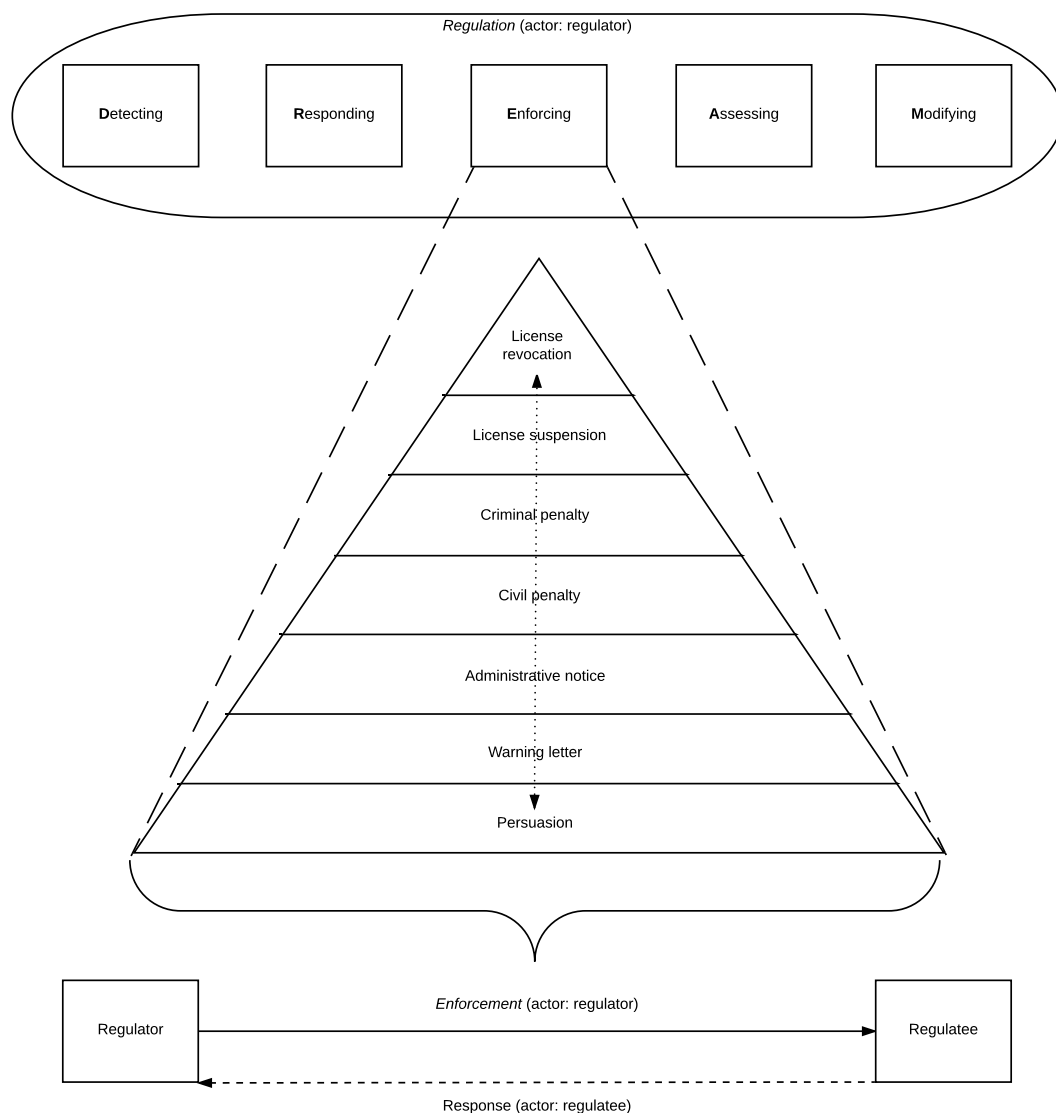


Figure 2. Overview of the theoretical model

3 Methodology

3.1 Research design

To answer the research question (§1.2) a single case study is performed with as main subject the Dutch DPA and its relevant enforcement activities in the period of 2015 through 2016. By performing document analysis, taking into account official reports, other related scientific or empirical work and media publications that shed light on the Dutch DPA and its enforcement activities in the period mentioned above, enough relevant data should be gathered to test the likelihood of a number of propositions. The to be tested propositions are derived from the theoretical framework, more specifically from the criticisms and reservations on responsive regulation. The propositions are formulated as followed:

1. *The Dutch DPA does not need to escalate through the layers of the enforcement pyramid because the currently deployed enforcement instruments are sufficient to reach the adequate level of compliance.*

The first proposition is a counterbalance to the other propositions. Although it is based on the theoretical framework it is not directly derived from the criticism on responsive regulation. The proposition entails that the mere threat of an available ‘deterrence’ approach could make it unnecessary for the Dutch DPA to escalate through the enforcement pyramid, away from a currently more ‘compliance’ oriented approach. This proposition is analysed first because if it is accepted, there is no need to proceed with the analysis of the other propositions.

2. *The Dutch DPA lacks the resources –i.e. fte’s and budget– to be able to escalate through the layers of the enforcement pyramid.*

This proposition is derived from the fifth criticism, which states that a regulators’ level of resources could result in a situation where it chooses not to escalate through the layers of the enforcement pyramid.

3. *The Dutch DPA lacks the right instruments –i.e. stick and impact too big or too small– to be able to escalate through the layers of the enforcement pyramid.*

This proposition is derived from the sixth criticism, which states that legislators can have provided the regulator with inadequate instruments, too severe or too minimal, to allow for a progression along the enforcement pyramid.

4. *The Dutch DPA operates with a level of discretion high enough to prevent it from escalation through the layers of the enforcement pyramid, raising issues of consistency of treatment across different regulatees, i.e. inequality and fairness.*

This proposition is derived from the seventh criticism, which states that high levels of discretion within the regulatory process can refrain regulators from escalating through the enforcement pyramid.

5. *The Dutch DPA has to enforce a standard (the applicable privacy law), which is –perceived to be– vague, or susceptible to interpretation, preventing escalation through the layers of the enforcement pyramid.*

This proposition is derived from the fifth criticism, which states that the kind of standards imposed (and how these are received) is a factor influencing whether escalating through an enforcement pyramid is optimal.

3.2 Justification

A single case study is chosen as the methodology for this research because it allows for an in-depth study of a case in its natural setting and its complexity in order to shed light on the broader social phenomenon of regulating behaviour within society (Yin, 2014, p. 3-23). A comparative case study has been considered, which would have included DPAs from other European member state countries, in this case Belgium (*Commissie voor de bescherming van de persoonlijke levenssfeer*) and Germany (*Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*) next to the Dutch DPA. These European countries were expected to have similar dynamics regarding the evolution towards more restricting privacy laws under influence of European legislation. Therefore their DPAs and their context would seem comparable

to the Dutch case, but a more detailed investigation proved different. The Belgian and German DPAs are organised in a far more decentralized manner, where – geographically– regionalized or sectorial –per industry organised– subcommittees are enforcing within their specific domains. The Dutch DPA organisationally only differentiates on the public and private sector, not resembling a similar decentralized structure, prohibiting a valid comparison. From a practical perspective, time is another factor reducing the possibility to conduct a comparative case study, due to the fact that reports and media publications regarding enforcement of privacy law in one or more additional countries would have to be added to the workload. This effect is reinforced by the fact that the German and Belgian DPAs have constructed their own specific ways of reporting, resulting in significant differences regarding the annual reports of the agencies involved, which would make a valid comparison highly unlikely. On top of this the German DPA reports only in German, which would additionally have required a translation effort. The translation issue is valid for most other options within the population of European member states. So after a solid consideration balancing the strengths and weaknesses of single and comparative case studies, taking into account practicalities and the time given to finish the research, the choice is made for a single, or holistic, case study.

The timespan chosen to conduct the research is the result of a scoping effort to keep the size of the project manageable and the gathered data as actual as possible. A dominant factor for the decision to start the time span at the 1st of January 2015 is that this is exactly one year before the introduction of the obligation to report data leakages to the Dutch DPA and its authority to –directly– impose relatively large fines. From the 1st of January 2016 onwards an increase in enforcement activities (numbers and punitive character) was therefore expected, making it a distinct marking point to compare a timeframe of a year ‘before’ and a year ‘after’. Choosing the period of 2015 through 2016 will have created a total timespan of 24 months in the relative near past, to ensure the availability of an as actual as possible dataset. The chosen timespan will also allow for a comparison of official enforcement numbers of the Dutch DPA between the years 2015 and 2016.

The constructed propositions are based on the theoretical framework regarding enforcement within the broader concept of regulation. The presumption is that to optimize the likelihood of successful enforcement, regulators should be able to realize responsive regulation, i.e. have the ability to operate an explicit enforcement pyramid

allowing them to escalate and deescalate through the layers of the pyramid in a responsive manner in accordance to the regulatees' response. The propositions are constructed on theory regarding regulatory failure, which addresses the factors and situations in which regulators are unable to achieve responsive regulation due to the fact that they are reluctant, hindered, or unable, to operate an explicit enforcement pyramid as previously described.

3.3 Data gathering

To gather data the choice has been made for document analysis. This option is preferred because the Dutch DPA consistently produces annual reports that are comparable over time, next to the availability of other –media– publications, and scientific and empirical work on the topic of enforcement by the Dutch DPA. As interviews with officials of the Dutch DPA and representatives of the population of regulatees were considered, it quickly became clear that neither of these actors were very inclined to speak frank and freely about their activities regarding enforcement and compliance. If these parties would have agreed to interviews on these particular subjects, it seemed unlikely to generate data and information that was not already publicly available. For these reasons the option to conduct interviews was deemed unfeasible.

Data is therefore gathered by collecting and analysing the annual reports –and their annexes– on the website of the Dutch DPA, with an emphasis on the –at the time of writing– most recent years of 2015 and 2016. The relevant data within these reports consist of fact and figures regarding enforcement activities of the Dutch DPA and fact and figures regarding its organisational and budgetary resources. Other relevant publications on the website of the Dutch DPA, i.e. official press releases, have also been collected and analysed regarding enforcement activities and resources. In addition, media publications were collected by scrutinizing the media predominantly via the internet on the topic of enforcement activities of the Dutch DPA. Over the period from September 2016 through December 2017, the search engine Google has been used to search for news clippings and other –relevant– articles. In this period, on an average frequency of every two weeks, several hours were spent searching via Dutch key words as: '*Autoriteit Persoonsgegevens*' (Dutch DPA), '*handhaving*' (enforcement), '*privacy*' (privacy), '*wet*' (law), '*rechtszaak*' (court case), '*naleving*' (compliance) and '*Wet bescherming persoonsgegevens*' (Dutch Data Protection Act).

The keywords were used in various combinations, including synonyms, antonyms and grammatical conjugations. A total of ninety-two initially collected documents were downloaded and saved or bookmarked in a browser. The decision whether a collected document was suitable for this research was based on the iterative process of skimming, reading and interpretation of each document (Bowen, 2009, p. 32). This process led to a total of thirty-seven documents used in this research, which are listed –amongst others– in the references, consisting of: eleven administrative documents, five formal studies, eighteen news clippings and three other articles. To extract data from the suitable documents the interview technique has been used for analysis, treating the documents as if they were respondents (O’Leary, 2004, p. 179-180). The document analysis was performed in a chronological manner in order to support a comparison between the years 2015 and 2016.

3.4 Operationalization

To operationalize the theoretical framework, including the constructed propositions, the enforcement instruments available to the Dutch DPA are mapped on the different layers of the more conceptual enforcement pyramid. This creates insight into what extent an explicit enforcement pyramid is available to the Dutch DPA. Next is to ascertain to what extent the Dutch DPA is able to operate the available enforcement pyramid. The mere fact that certain tools are available does not automatically mean that the Dutch DPA uses them, even in cases where it would be entitled to do so. Investigating the cause(s) of the extent to which the Dutch DPA can, or is willing, to escalate along the enforcement pyramid is realized by testing the likelihood of the constructed propositions. This results in the situation where it is possible to answer the research question.


Enforcement pyramid	Instruments Dutch DPA	Coercive nature
License revocation	(N/A)	
License suspension	(N/A)	
Criminal penalty	Criminal fine	
Civil penalty	Directly imposable administrative fine Order subject to non-compliance penalty	
Administrative notice	Official investigation	
Warning letter	Warning letter	
Persuasion	Verbal warning Questions & Tips Contact with the media	

Figure 3. Instruments of the Dutch DPA mapped on the enforcement pyramid

The table in figure 3 shows how the instruments available to the Dutch DPA are mapped on the layers of the enforcement pyramid. The three layers from the bottom up correspond with the ‘compliance’ approaches as introduced in §2.2.2. The four layers at the top correspond with the ‘deterrence’ approaches and it has to be emphasized that the top two layers ‘license suspension’ and ‘license revocation’ are not –yet– available to the Dutch DPA. An overview of the operationalized theoretical model regarding enforcement is presented in figure 4.

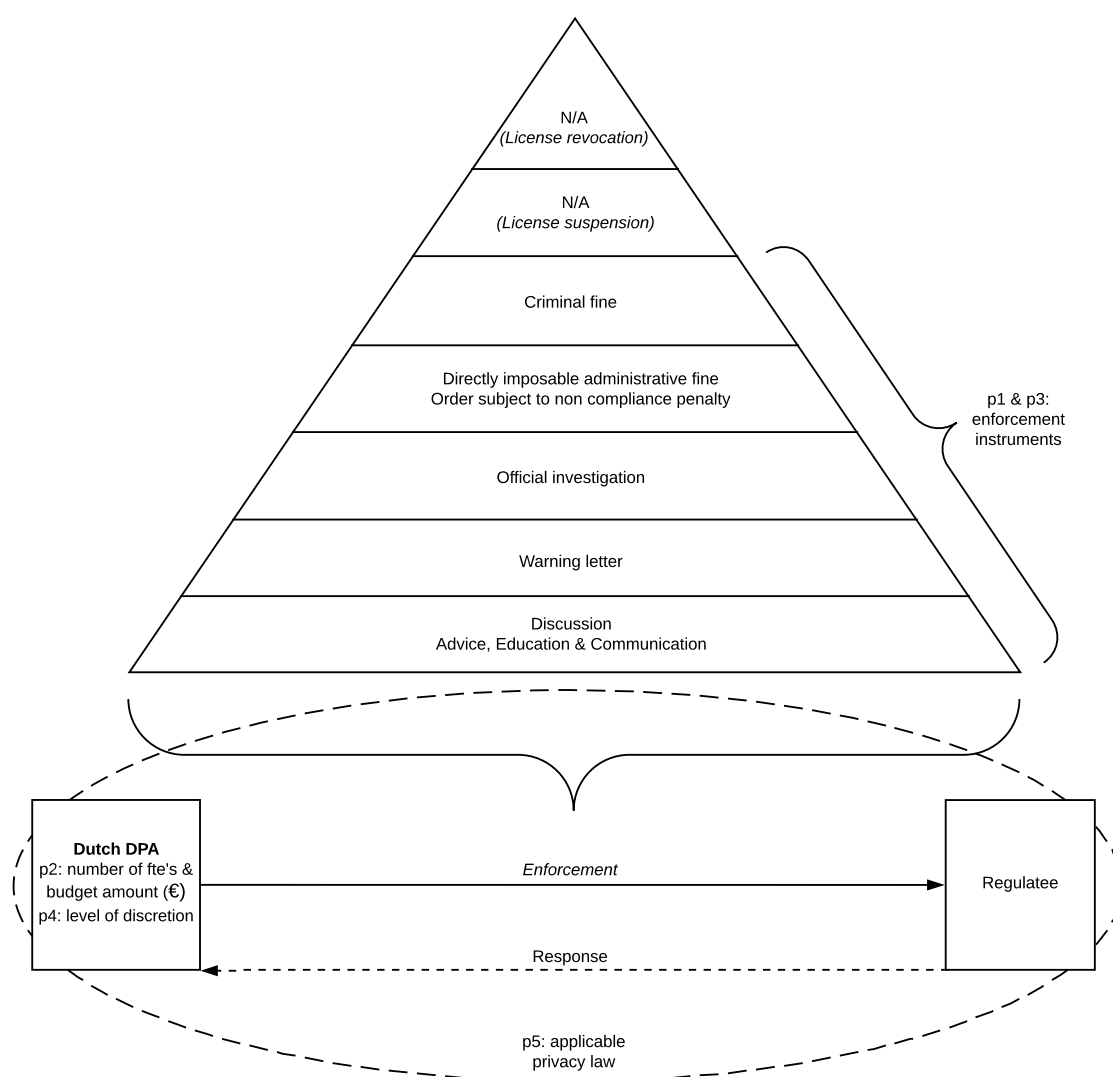


Figure 4. Overview of the operationalized theoretical model

Figure 4 shows the enforcement pyramid available to the Dutch DPA, with its own specific layers increasing in coercive, or deterring, character towards the top. The propositions ‘p1’ through ‘p5’ have been added to the diagram at positions illustrating

their relation to the theoretical model. The propositions can be expressed as variables and according to the theoretical framework, these variables are expected to have an influence on the enforcement capabilities of the Dutch DPA, i.e. the extent to which it is able to operate an explicit enforcement pyramid. The –expected– causal relations between the dependent and independent variables in the theoretical model are expressed in figure 5.

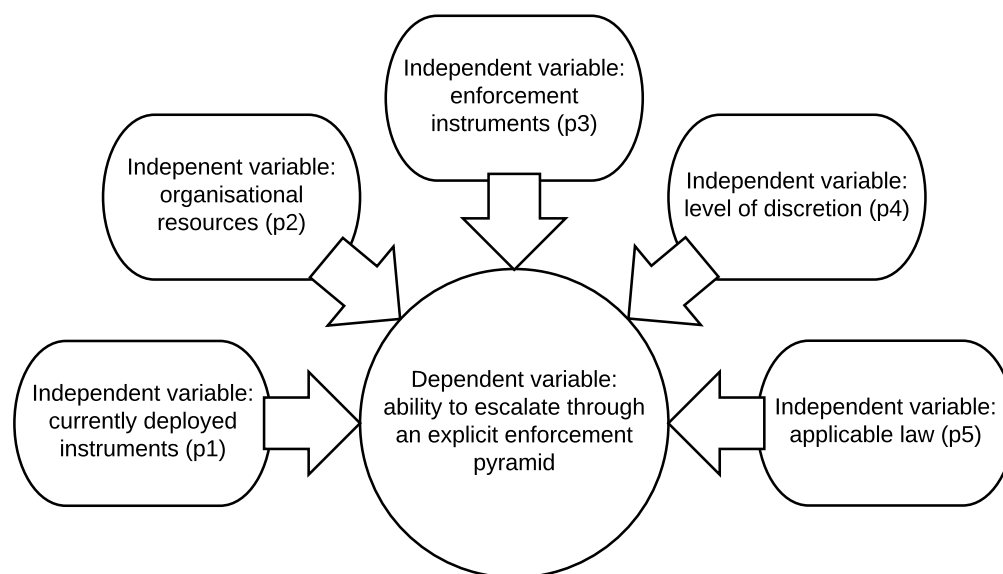


Figure 5. Overview of the variables

The introduction of this research illustrates that during the chosen timespan there has been a low level of coercion in the enforcement of the applicable privacy law in the Netherlands. This low level of coercion used by the Dutch DPA is illustrated in figure 1 (§1.1), which shows that the Dutch DPA has not been using all of the available enforcement instruments. This corresponds with what from the theoretical framework can be defined as the ability to escalate through an explicit enforcement pyramid. The aim of this research is to find an explanation for the specific situation regarding the Dutch DPA, which has been unable –or at least had the limited ability– to operate an explicit enforcement pyramid. This research strives to find an answer to the research question by testing the propositions, i.e. the relation between the independent and dependent variables.

The following subparagraphs will provide the operationalization of the independent variables ‘p1’ to ‘p5’ in order to commence with the analysis.

3.4.1 Currently deployed instruments

In order to measure the variable ‘currently deployed instruments’, derived from the first proposition ‘p1’, the currently deployed enforcement instruments available to the Dutch DPA will be expressed in the frequency of deployment on an annual basis. The annual numbers, corresponding with the chosen timespan for measurement during this research, will be linked to normative expressions gathered during the document analysis: statements by relevant actors regarding the effectiveness of currently deployed instruments and the deterring effect of the available –but up to now unused– more coercive instruments. This should lead to an indication of the likelihood of the proposition stating that the Dutch DPA does not need to escalate through the enforcement pyramid because the currently deployed enforcement instruments are sufficient to reach the adequate level of compliance. The interview questions used to analyse the selected documents are:

- 1. What are the currently deployed instruments by the Dutch DPA, i.e. respective frequency of use on an annual basis, during the chosen timespan of this research?*
- 2. How do the currently deployed instruments by the Dutch DPA, i.e. respective frequency of use on an annual basis, affect its ability to perform its tasks?*

3.4.2 Organisational resources

To measure the variable ‘organisational resources’ of the Dutch DPA, which is derived from the second proposition ‘p2’, it will be expressed as the number of fte’s and the budget in euros available to the Dutch DPA on an annual basis. The annual numbers, corresponding with the timespan chosen for measurement during this research, will be linked to normative expressions gathered during the document analysis: statements by relevant actors regarding the organisational resources in relation to the ability of the Dutch DPA to enforce the applicable privacy law. This should lead to an indication of the likelihood of the proposition stating that the Dutch DPA lacks the resources to be able to escalate through the layers of the enforcement pyramid. The interview questions used to analyse the selected documents are:

3. *What are the organizational resources, i.e. the number of fte's and annual budget, of the Dutch DPA during the chosen timespan of this research?*
4. *How do the organisational resources of the Dutch DPA affect its ability to perform its tasks?*

3.4.3 Enforcement instruments

In order to measure the variable 'enforcement instruments', derived from the third proposition 'p3', the enforcement instruments available to the Dutch DPA will be expressed according to their punitive character and their respective frequency of use on an annual basis. The annual numbers, corresponding with the chosen timespan for measurement during this research, will be linked to normative expressions gathered during the document analysis: statements by relevant actors regarding the use –and impact– of the enforcement instruments available to the Dutch DPA. This should lead to an indication of the likelihood of the proposition stating that the Dutch DPA lacks the right instruments –impact too big or too small– to be able to escalate through the layers of the enforcement pyramid. The interview questions used to analyse the selected documents are:

5. *What are the enforcement instruments of the Dutch DPA, i.e. kind of instruments and their respective frequency of use on an annual basis, during the chosen timespan of this research?*
6. *How do the enforcement instruments of the Dutch DPA affect its ability to perform its tasks?*

3.4.4 Level of discretion

To measure the variable 'level of discretion', derived from the fourth proposition 'p4', the gathered documentation will be scrutinized to identify information, including normative statements by relevant actors, regarding the existence of a level of discretion used by the Dutch DPA and its impact on the enforcement process during the chosen timespan of measurement for this research. This should lead to an indication of the likelihood of the proposition stating that the Dutch DPA operates with a level of discretion high enough to prevent it from escalation through the layers

of the enforcement pyramid, raising issues of consistency of treatment across different regulatees. The interview questions used to analyse the selected documents are:

7. *Is there a level of discretion existent in the modus operandi of the Dutch DPA during the chosen timespan of this research?*
8. *How does the existent level of discretion used by the Dutch DPA affect its ability to perform its tasks?*

3.4.5 Applicable law

To be able to measure the variable ‘applicable law’, derived from the fifth proposition ‘p5’, the gathered documentation will be scrutinized on information, including normative statements by relevant actors, regarding the level in which the Dutch Data Protection Act can be identified as an open standard, or its susceptibility to interpretation, during the chosen timespan of measurement for this research. This should lead to an indication of the likelihood of the proposition stating that the Dutch DPA has to enforce a standard (the applicable privacy law), which is –perceived to be– vague, or susceptible to interpretation, preventing escalation through the enforcement pyramid. The interview questions used to analyse the selected documents are:

9. *What kind of standard –open or concrete–, i.e. applicable privacy law, does the Dutch DPA has to enforce during the chosen timespan of this research?*
10. *How does the kind of standard, i.e. applicable privacy law, the Dutch DPA has to enforce affect its ability to perform its tasks?*

3.5 Validity and reliability

To establish the quality of the research design used in this thesis the construct validity, internal validity, external validity and reliability will be discussed in this paragraph.

The construct validity sets out to identify the correct operational measures for the concepts being studied (Yin, 2014, p 46). As the operationalization has shown, the propositions –after being derived from theory– are expressing as independent variables and are going to be tested by two questions corresponding to each

proposition. The first of each pair of questions is used to measure the variable expressed as a quantitative or qualitative parameter during the timeframe of this research and the second question to ascertain a relationship between the independent variable and the dependent variable. Multiple sources of evidence related to the case of this research created by different actors have been used: administrative documents, formal studies and news clippings and other articles predominantly available via the internet. A chain of evidence has been provided in the reference section of this thesis, where all sources –and if applicable their digital locations of retrieval– have been listed.

The internal validity seeks to establish causal relationships, which is relevant for this research as it is explanatory (Yin, 2014, p. 47). This research strives to build explanations during the analysis phase by testing five propositions. Combined with the addition of a rival –or counterbalancing– explanation (p1) in the set of propositions, the internal validity of this research is strengthened.

The external validity defines the domain to which the findings of this research can be generalized (Yin, 2014, p. 48). Due to the fact that this is a single case study the external validity of this research is limited. Although this research relies on an extensive theory regarding regulation and enforcement, the findings are limited to the regulation of privacy in the Netherlands. If a multiple case study including other EU member state-DPAs had been feasible, the generalizability of the results would have been less limited.

The reliability of a research demonstrates that its operations can be repeated with the same results (Yin, 2014, p. 48). The methodology of this research has been made transparent in the current chapter and all the used sources are retrievable due to the fact that they are available on the internet as open sources. Even though the author of this thesis strived to be extensive in his data gathering, it might be that there is relevant data available the author has missed and therefore has not been able to analyse. The chance of missing relevant data is however deemed small due to the fact that over the period of September 2016 through December 2017, on an average frequency of every two weeks, several hours were spent extensively searching the internet via various relevant Dutch key words (§3.3). In addition, the chance that possibly missed data within the same timeframe of this research would lead to significantly different outcomes is deemed to be small as well.

4 Analysis

Before the analysis is conducted, the next paragraph will provide a brief description of the applicable privacy law in the Netherlands and the subject of this research: the Dutch DPA and its working method.

4.1 The applicable law and the Dutch DPA

On the 6th of July 2000 Dutch government introduced the Dutch Data Protection Act (Wbp) to safeguard the ways in which personal information can be processed. The Dutch Data Protection Act is the applicable law for regulating privacy in the Netherlands since. Due to the broad definitions of ‘personal information’ and ‘processing of personal information’ (see §2.1.1) it is hard to imagine actors operating within Dutch jurisdiction to whom the Dutch Data Protection Act would not be applicable. Most of the articles in the Dutch Data Protection Act are derived from the European Directive 95/46/EC, which strives for more harmonisation of data protection within the EU. As a reaction to the fragmented enforcement of privacy laws within the EU and the fast paced technological developments, the European Commission (EC) proposed for an European general regulation regarding data protecting at the beginning of 2012. On the 26th of April 2016, after an intensive legislative process, the General Data Protection Regulation (GDPR) was adopted. On the 25th of May 2018 the GDPR will be enforced, abolishing the European Directive 95/46/EC and all national privacy laws within the EU, including the Dutch Data Protection Act (*Nederlands Tijdschrift voor Europees Recht*, 2017 [6], p. 157-158).

Without going into much detail or claiming to be complete, some of the more relevant aspects of the currently applicable privacy law in the Netherlands, the Dutch Data Protection Act (Wbp), will be discussed next. If an organisation processes personal information it can only do so based on legal grounds and/or an in advance defined, concrete and justified goal. The processing of personal information should be limited to fit this goal and it is prohibited to process more personal information than necessary in accordance with the previously mentioned legal grounds and/or clearly defined goal. Next to that, personal information should not be retained longer than necessary and protocols, processes and technical procedures should enable the timely and irretrievable erasure of obsolete personal information. Organisations should process personal information at an adequate level of organisational and technical security, not only against threats from outside the organisation but to internal threats

as well, e.g. unauthorized access by employees or unnecessary irreversible corruption or destruction due to internal –technical– failures. In that respect, sensitive personal information should be protected at even higher levels of security. In the case an organisation has –partially– outsourced the processing of personal information to a third party there should be a formal, legal agreement in place between both parties to ensure compliance to privacy law in such constructions. Organisations are obliged to report data leakages regarding personal information within seventy-two hours to the Dutch DPA and under certain circumstances to the individuals of whom personal information has leaked as well. The Dutch Data Protection Act strives to protect the rights of the individuals involved –the data subjects– via articles covering their consent, their right to correct or erase personal information and the ways in which they are informed about the processing of their personal information. Through the entire process organisations should be able to demonstrate their compliance to the applicable privacy law, which predominantly entails creating an auditable trail of the relevant effort and results with respect to their compliance (NOREA, *Privacy Impact Assessment version 1.2*, 2015).

The regulator, or enforcer, of the applicable privacy law in the Netherlands is the Dutch DPA, which is an independent governmental organisation operating under the political responsibility of the Dutch Minister of Justice and Security. As an independent governmental organisation the Dutch DPA can operate with a certain degree of autonomy in relation to the Dutch ministry of Justice and Security (*Nederlands Tijdschrift voor Europees Recht*, 2017 [6], p. 157-158).

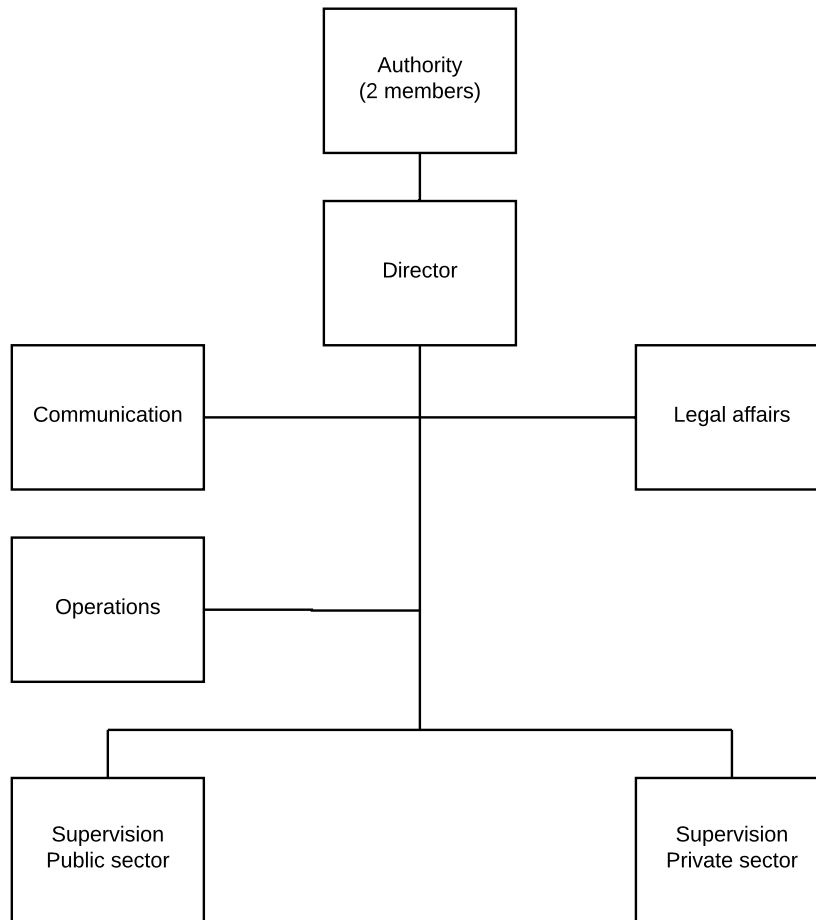


Figure 6. Organisational structure of the Dutch DPA

Figure 6 shows the organisational structure of the Dutch DPA. The most recent annual report indicates that the organisational size is around 72 fte's and the annual budget is just over eight million euro (AP, *Bijlage jaarverslag 2016*, p. 3,4 & 12).

The working method of the Dutch DPA consists of supervision regarding the processing of personal data in order to ensure compliance with the applicable law. In order to encourage compliance the Dutch DPA uses a mix of instruments. When investigating alleged infringements of the law, the Dutch DPA needs to decide which next steps to undertake. It uses several criteria to determine if an investigation will be conducted, depending for example on: whether there is a suspicion of serious and structural violations that affect many people; whether the Dutch DPA can make a difference based on its capabilities; and whether the violations fall within the annual themes set by the Dutch DPA. Next to conducting investigations, the Dutch DPA can also act by sending warning letters and entering into discussions. This is done predominantly in cases where the previously mentioned criteria are not met. If the

violation continues, or starts again after some time, the Dutch DPA can still conduct an investigation. In the situation where violations persist, the Dutch DPA has the ability to impose an order subject to non-compliance penalty. In such a case, a violator of the law will be given a certain period of time to become compliant after which a fine will have to be paid if the regulatee remains non-compliant. As mentioned before, since the 1st of January 2016 the ability of the Dutch DPA to – directly– impose fines has been significantly expanded. Next to the more coercive instruments, communication is an important instrument to encourage compliance with the law. The Dutch DPA maintains contact with the media and engages in discussions with trade organisations and other stakeholders. It also provides lectures, presentations and other events on a regular basis alongside the provision of information via telephone consultation hours and through its website (AP, *Jaarverslag 2015*; AP, *Jaarverslag 2016*).

4.2 Testing the propositions

To test the propositions ‘p1’ to ‘p5’ the interview technique for document analysis will be conducted in the following paragraphs (§4.2.1 to §4.2.5). The interview technique utilizes questions 1 to 10, constructed in paragraph 3.4, to gather the relevant data and subsequently provide an interpretation. Each paragraph will conclude with the respective results and paragraph 4.3 will provide an overview of the likelihood of the tested propositions.

4.2.1 Currently deployed instruments

Proposition ‘p1’ stating that the Dutch DPA does not need to escalate through the enforcement pyramid because the currently deployed enforcement instruments are sufficient to reach the adequate level of compliance, will be analysed regarding its likelihood in this paragraph. This is a counterbalancing proposition, which entails that the mere threat of an available ‘deterrence’ approach could make it unnecessary for the Dutch DPA to escalate through the enforcement pyramid, away from a currently more ‘compliance’ oriented approach. The question to be answered is:

- 1. What are the currently deployed instruments by the Dutch DPA, i.e. respective frequency of use on an annual basis, during the chosen timespan of this research?*

Figure 7 shows the currently deployed instruments by the Dutch DPA, i.e. the enforcement instruments actually used by the Dutch DPA during the chosen timespan of this research. The sources of this information are the Dutch DPA's annual reports, including annexes, of the years 2015 and 2016.

Instruments Dutch DPA	2015	2016
Order subject to non-compliance penalty	17	20
Official investigation	48	197
Warning letter	226 (N/S)	157
Verbal warning	226 (N/S)	146
Questions & Tips	7210	9277
Contact with the media	617	797

Figure 7. Enforcement instruments currently deployed by the Dutch DPA (AP, Bijlage jaarverslag 2015, p. 6, 10-11; AP, Bijlage jaarverslag 2016, p. 5, 9-11)

There is a slight increase in orders subject to non-compliance penalty in 2016. As a result of the introduction of the obligation to report data leakages to the Dutch DPA, there has been a significant increase in the amount of official investigations in 2016. The total number of warnings (verbal and officially by letter) has increased as well as the category questions & tips. It has to be emphasized that the Dutch DPA started reporting for the first time about issued warnings in 2015, at that time not specifying whether they were verbal or by official letter. The least coercive instrument in the enforcement pyramid, being contact moments with the media for generic communication and informing of the public, have also increased.

Overall the analysis shows that the currently deployed enforcement instruments did not see any changes regarding their nature during the chosen timespan of this research, i.e. they remained unaltered. There was a relatively small increase in their frequency of use in 2016 when compared to 2015, which can predominantly be contributed to the introduction of the obligation to report data leakages at the 1st of January 2016.

This leads to the following question:

2. *How do the currently deployed instruments by the Dutch DPA, i.e. respective frequency of use on an annual basis, affect its ability to perform its tasks?*

The fact that the nature of the currently deployed instruments has not changed and that they have seen a relatively small increase in deployment over the years 2015 and 2016 could indicate that this constellation of currently deployed instruments is sufficient for the Dutch DPA to perform its tasks. The analysis will start with addressing the ability of the Dutch DPA to perform its task in a more generic sense, namely its ability to achieve compliance and its ability to enforce.

Regarding the level of compliance to the applicable privacy law in the Netherlands, reports and studies indicate the level of compliance to be low. In her annual report of 2015, the Dutch DPA, states that the self-perceived need to act in accordance with the applicable privacy law seems limited. It appears to the Dutch DPA that there are insufficient external incentives to prevent violations of privacy law: violations being reported by consumers are rare and the chance of being caught by the Dutch DPA is perceived to be very small (AP, *Jaarverslag 2015*, p. 6-7). In the year 2016 twelve per cent of Dutch organisations were fully complaint to the obligation to report data leakages and ninety-five per cent of Dutch organisations were not –preparing to be– compliant to the GDPR (*Centric Security Survey 2016*, p. 11). Another study, published in June 2017, shows that forty-nine per cent of Dutch organisations stated to be compliant to the obligation to report data leakages and, amongst other aspects showing low levels of compliance to Dutch privacy law, forty-eight per cent of Dutch organisations do not expect to be compliant to the GDPR once it will be enforced on the 25th of May 2018 (PricewaterhouseCoopers, *Privacy Governance onderzoek 2017*, p. 6). The low level of compliance to privacy law in the Netherlands as illustrated above, seems to coexist with –and most likely is the result of– a low level of enforcement by the Dutch DPA. Several items in the media illustrate a Dutch DPA incapable of performing her tasks leading to a number of occasions in which Dutch courts demanded enforcement by the Dutch DPA (see www.zorgictzorgen.nl, *Autoriteit Persoonsgegevens verre van waaks als privacy-waakhond* [18th of May 2017]; www.privacybarometer.nl, *Rechter geeft Autoriteit Persoonsgegevens er van langs* [17th of July 2017]; www.computable.nl; *Rechter: AP reageert te laks op*

schendingen privacy [19th of July 2017]; Rechtbank Midden-Nederland [2017] *AWB – 16 _ 3326 & AWB – 16 _ 4199*; Rechtbank Gelderland [2017] *AWB – 17 _ 2340*).

The above illustrates that there is a low level of compliance and a low level of enforcement regarding the applicable privacy law in the Netherlands (which would imply that to a certain extent the Dutch DPA is not able to perform its task). It could be that the Dutch DPA is relying on the deterring effect of its most coercive instruments without having to use them to increase compliance to the applicable privacy law. When combined with the currently deployed instruments, this would mean the Dutch DPA would never have to escalate further than the ‘order subject to non-compliance penalty’. This would only work if the regulatees are ignorant of this strategy and truly believe that a fine eventually will be imposed on them. The line of thought, formulated above, is illustrated by an article regarding the expanded authority by the Dutch DPA to impose fines, which states: *“The Dutch DPA says that it predominantly values the preventive effect of its authority to impose fines. The expectation is that the authority to impose fines will stimulate companies and governmental organisations to attend to the security of personal information at an earlier stage. This should prevent privacy violations. If a violation of the Dutch Data Protection Act is intentional or the result of grave negligence, the supervisor is able to directly impose a fine. In all other cases this is preceded by an injunction”* (Security.nl, 2016, para. 2).

In an interview chairman Aleid Wolfsen reacts to the fact that the British DPA had, shortly before the interview, imposed fines: *“We have a whole series of data leakages, we now have dozens of cases under investigation, so this is going to happen here as well ... Those fines are coming!”* (NU.nl, 2017, section *Boetes*). This quote indicates that the Dutch DPA is promoting its expanding authority to impose fines. It can be interpreted as the execution of the aforementioned deterrence strategy to achieve more compliance.

An article regarding a recently issued ‘order subject to non-compliance penalty’ to Facebook by the Dutch DPA states: *“The fine of several million euro currently risked by Facebook for violating the Dutch Data Protection Act is insignificant next to what the Dutch DPA can impose next year. If the Dutch DPA would then, as she did two weeks ago, conclude that the social media platform on multiple points does not specifically inform her users about the use of personal information she can impose a maximum fine of several billions in euros”* (FinancieelDagblad.nl, 2017, para. 1). This

quote is another example of a situation in which the Dutch DPA is promoting its expanding authority to impose fines and can also be interpreted as the execution of the aforementioned deterrence strategy to achieve more compliance. Continuing in the same article, Aleid Wolfsen warns: *“This could turn out to be very unpleasant for companies ... Wrong is wrong ... We want companies to respect the privacy law ... The fines are imposed per violation ... And we don not apply quantity discounts”* (FinancieelDagblad.nl, 2017, para. 2). This statement reinforces the previously identified promotion of the expanded authority to impose fines by the Dutch DPA, which aligns with the deterrence strategy to achieve more compliance.

The analysis shows that the Dutch DPA seems to promote its expanding authority to impose fines while sticking to the currently deployed instruments. This could indicate that it is adhering to the previously discussed deterrence strategy and the currently deployed instruments are sufficient for it to perform its task. Nevertheless the discussed deterrence strategy, by threatening with fines while the Dutch DPA only relies on its currently deployed instruments to achieve compliance, remains speculative. Moreover, as illustrated previously in this paragraph the Dutch DPA has been unable to fully perform its tasks due to the perseverance of a low level of compliance and a low level of enforcement over the chosen timespan of this research.

Results ‘current instruments’

In answer to question 1, analysis shows that the currently deployed instruments by the Dutch DPA have hardly changed in frequency of use over the chosen timespan of this study. A relatively small increase in the frequency of use of certain currently deployed instruments was identified, which predominantly was the effect of the introduction to report data leakages under the Dutch Data Protection Act on the 1st of January 2016.

In answer to question 2, the analysis has shown that there is a persistent low level of compliance and a low level of enforcement regarding privacy regulation in the Netherlands. This emphasises the necessity of a regulator making use of its ability to escalate through the entire explicit enforcement pyramid available to it. Therefore, even if the Dutch DPA would have adopted the speculative deterrence strategy and is only relying on its currently deployed instruments while threatening to impose fines, meaning that it willingly does not utilize its ability to escalate through the entire explicit enforcement pyramid, this strategy has failed during the chosen timespan for

this research and the Dutch DPA has to a certain extent been unable to perform its tasks.

4.2.2 Organisational resources

This paragraph sets out to analyse the likelihood of proposition ‘p2’ stating that the Dutch DPA lacks the resources –i.e. fte’s and budget– to be able to escalate through the layers of the enforcement pyramid. This proposition is derived from the fifth criticism, which states that a regulators’ level of resources could result in a situation where it chooses not to escalate through the layers of the enforcement pyramid. The question to be answered is:

3. *What are the organizational resources, i.e. the number of fte’s and annual budget, of the Dutch DPA during the chosen timespan of this research?*

Resources Dutch DPA	2015	2016
Number of fte's	72,5	72,5
Budget amount in euros (€)	8,2 M	8,1 M

Figure 8 Organisational resources of the Dutch DPA (AP, Bijlage jaarverslag 2015, p. 3-5; AP, Bijlage jaarverslag 2016, p. 3-4)

According to the figure (8) above, the number of fte’s and the budget of the Dutch DPA remain at a constant level over the years of 2015 and 2016. This is striking to see when realizing that at the 1st of January 2016 the obligation to report data leakages regarding personal information came in to effect, next to the expansion of the Dutch DPA to impose fines. These developments were expected to lead to an increased workload of the Dutch DPA, which in turn would demand more organizational resources. The question to be answered here is:

4. *How do the organisational resources of the Dutch DPA affect its ability to perform its tasks?*

In a news article regarding the understaffing of the Dutch DPA the previous chairman of the Dutch DPA, Jacob Kohnstamm, states the following: *“I have been unable to convince the Ministry of increasing the human resources in order to perform the new*

tasks. Therefore I look forward with fear to the start of the obligation to report data leakages” (NRC Handelsblad, 2015, section *Angstig uitkijken*). This means that in 2015 the Dutch DPA realized it had insufficient resources to be able to perform its tasks after the –at that time– imminent introduction of the obligation to report data leakages regarding personal information. The Dutch DPA was unsuccessful at convincing Dutch political decision makers to increase its organisational resources in accordance with the expected increase in workload. After the article states the numbers of organizational resources, corresponding with the numbers of 2015 in figure 8, Kohnstamm replies: *“I think the fivefold of the current numbers would be a good start. Not only because of the obligation to report data leakages and the European rules, but also due to the fact that personal information is the new gold. Everyday you see dozens of new apps and websites”* (NRC Handelsblad, 2015, section *Angstig uitkijken*). This shows that at that time the Dutch DPA expected a significant increase in workload, not only as the result of intensified legislation but also due to the fact that processing of personal information was a fast growing –business– activity in society. In the same article Kohnstamm implies that the lack of human resources will possibly have a big impact on the enforcement of privacy law: *“Already we have to manage expectations. Meaning that we have to be very selective. We can’t handle more than fifteen to twenty cases per year in this way. This means that on a very regular basis we have to let cases go”* (NRC Handelsblad, 2015, section *Maximaal vijftien tot twintig grote zaken mogelijk*). We can infer from this that in 2015 the Dutch DPA was already dealing with a negative impact on its ability to perform its task due to a lack of organisational resources, regardless of the –at that time– imminent introduction of the obligation to report data leakages regarding personal information. The negative impact concretely entails that in 2015 the Dutch DPA was limited in the number of cases it could handle per year, resulting in situations where cases were being dropped on a regular basis.

In another interview the previous chairman of the Dutch DPA was asked if the Dutch DPA was adequately equipped to perform its supervisory tasks. His answer was: *“The size of the Dutch DPA is too limited for sure”* (Audit Magazine, 2016, [1], p. 8). This statement indicates that also in 2016 the organizational resources of the Dutch DPA were insufficient for it to perform its tasks.

In an article by Bits of Freedom the start of the newly appointed –current– chairman of the Dutch DPA, Aleid Wolfssen, on the 1st of August 2016 was discussed. In this

column style article the new chairman was provided with the unsolicited advice: *“Demand more budget and human resources ... the budget and human resources of the Dutch DPA are insufficient for its tasks. With slightly more than eight million euro and a little over 70 fte it is impossible for the Dutch DPA, after the adoption of the European privacy law [i.e. GDPR], to completely and effectively perform her tasks”* (Bits of Freedom, 2016, section 4. *Pleit voor meer budget en mankracht*). This illustrates that in 2016 the opinion of privacy interest groups supported the notion that the Dutch DPA had insufficient organisational resources to perform its tasks, especially in the light of the anticipated European privacy law.

In an interview with the current chairman of the Dutch DPA, Wolfsen states: *“I admit that at the present we cannot do much as watchdog ... We are going to change in the coming years. The minister has announced an independent, external and objective study about what the new Dutch DPA will look like once the European privacy law comes into effect, and what budget we will have. I am content with that. I am awaiting this study, before I am going to complain that our budget should be significantly increased”* (Trouw, 2016, para. 12). Given this statement, it is clear that in 2016 Dutch political decision makers had been triggered to start a study regarding the organisational resources of the Dutch DPA in order to adapt to the expected increased workload due to the anticipated European privacy law coming in to effect. The statement also indicates that at that time the organisational resources were already insufficient for the Dutch DPA to perform its task, but the announced study was sufficient for the chairman of the DPA to refrain from complaining about the situation.

The results of the study referred to by Wolfsen in Trouw (2016) were sent to Dutch parliament on the 31st of May 2017 (*Ministerie van Veiligheid en Justitie*, 2017, p. 1-2). The report concluded that from May 2018 onwards, when the European privacy law comes into effect, the Dutch DPA needs a significant increase in budget and human resources depending on three scenario's: low, medium and high (Andersson Elffers Felix [AEF], 2017, p. 3-4). These three scenarios are added to the numbers of figure 8 leading to an overview in figure 9 below.

Resources Dutch DPA	2015	2016	<i>scenario low</i>	<i>scenario medium</i>	<i>scenario high</i>
Number of fte's	72,5	72,5	185,3	222,4	270,7
Budget amount in euros (€)	8,2 M	8,1 M	19,6 M	23,7 M	29,4 M

Figure 9. Future scenarios organisational resources of the Dutch DPA

In a later interview chairman Wolfsen of the Dutch DPA is asked if the enforcement, needing a lot of manpower and ICT knowledge, is going to be a problem. He answers: *“We do not know yet. Up to this moment we were too small and vulnerable ... When the task forthcoming from the obligation to report data leakages was added, we did not see an increase in additional staff ... An external independent study showed what our size should be in order to adequately enforce the GDPR. The result was that we should be 2,5 to 3,5 times the size we are now. At this moment we have around 90 employees. Parliament and the Ministry have granted us permission to start recruiting, which we are currently doing”* (ICT Magazine, 2017, para. 10). Combined with the scenarios of the previously mentioned study (figure 9), this indicates that the DPA has had insufficient organisational resources in 2015 and 2016 to perform its tasks and will need significant increases of its organisational resources to be able to perform its tasks when the European privacy law comes into effect.

Results ‘organisational resources’

In answer to question 3, analysis shows that the organisational resources of the Dutch DPA during the period of 2015 through 2016 remained at a constant level of 72 fte and an annual budget of just over 8 million euro.

In answer to question 4, the analysis shows that the level of organisational resources during the period of 2015 through 2016 was too low and therefore had a negative impact on the ability of the Dutch DPA to perform its tasks, i.e. its ability to operate – by (de)escalation– an explicit enforcement pyramid: without stating exact numbers the chairman of the Dutch DPA indicated they had to drop (enforcement)cases on a regular basis. The negative impact most likely increased after the 1st of January 2016, when the aforementioned changes in Dutch privacy law –as a prelude to the coming GDPR– created an increased workload for the Dutch DPA.

4.2.3 Enforcement instruments

In this paragraph an analysis is made of the likelihood of proposition ‘p3’ stating that the Dutch DPA lacks the right instruments –i.e. stick and impact too big or too small– to be able to escalate through the layers of the enforcement pyramid. This proposition is derived from the sixth criticism, which states that legislators can have provided the regulator with inadequate instruments, too severe or too minimal, to allow for a progression up the enforcement pyramid. The question to be answered is:

5. *What are the enforcement instruments of the Dutch DPA, i.e. kind of instruments and their respective frequency of use on an annual basis, during the chosen timespan of this research?*

Instruments Dutch DPA	2015	2016
Criminal fine	0	0
Directly imposable administrative fine	0	0
Order subject to non-compliance penalty	17	20
Official investigation	48	197
Warning letter	226 (N/S)	157
Verbal warning	226 (N/S)	146
Questions & Tips	7210	9277
Contact with the media	617	797

Figure 10. *Enforcement instruments used by the Dutch DPA (AP, Bijlage jaarverslag 2015, p. 6, 10-11; AP, Bijlage jaarverslag 2016, p. 5, 9-11)*

Figure 10 shows the number of instances on an annual basis in which the Dutch DPA has used the instruments within the available enforcement pyramid. Starting at the top of the enforcement pyramid, it is striking to see that the Dutch DPA has not used the instruments of –directly imposable– administrative and criminal fines in 2015 and 2016. There is a slight increase in orders subject to non-compliance penalty in 2016. The significant increase in the amount of official investigations in 2016 is the result of the introduction of the obligation to report data leakages to the Dutch DPA, which went into force at the 1st of January 2016. The total number of warnings (verbal and officially by letter) has increased, which could be a side effect of the increase in the category questions & tips due to the fact that tips about possible infringements – without specifying the exact number– are part of this category next to questions

asked. The Dutch DPA has stated in her annual reports that the aforementioned tips can result in warnings. It has to be emphasized that the Dutch DPA started reporting for the first time about issued warnings in 2015, at that time not specifying whether they were verbal or by official letter. The least coercive instrument in the enforcement pyramid, being contact moments with the media for generic communication and informing of the public, has also seen an increase. This first part of the analysis in the current paragraph resembles the first part of the analysis in §4.2.1 except for the fact that the criminal fine and directly imposable administrative fine are now included in the analysis.

Regarding the kind of enforcement instruments available to the Dutch DPA a major change was introduced to the Dutch Data Protection Act on the 1st of January 2016. From that time on the Dutch DPA had the authority to impose heavier fines on more types of non-compliance cases than before. The maximum fine was now relative instead of absolute, i.e. ten per cent of the annual revenue of a legal entity in case the absolute maximum of 820.000 euro was deemed insufficient by the Dutch DPA. Before the 1st of January 2016, the Dutch DPA could only impose a fine on non-compliance cases regarding two articles of the Dutch Data Protection Act. This was now significantly expanded with dozens of other articles (AP, *Boetebeleidsregels Autoriteit Persoonsgegevens* 2016, p. 3-12).

Acknowledging the aforementioned findings leads us to the following question:

6. *How do the enforcement instruments of the Dutch DPA affect its ability to perform its tasks?*

First of all, it is clear that the Dutch DPA has been provided with an explicit enforcement pyramid consisting of compliance and deterrence approaches. The expansion on the 1st of January 2016 of the authority to impose fines has changed the balance –or synergy– between the available compliance and deterrence approaches. The question is: for better or for worse? It seems that the proverbial stick before the 1st of January 2016 was deemed too small: *“The choice of the legislator to expand the authority to impose fines is the result of the desire to increase the sanction possibilities of the Dutch DPA in order to reach higher levels of compliance, by private as well as public organisations, to the Dutch Data Protection Act”* (AP,

Boetebeleidsregels Autoriteit Persoonsgegevens 2016, p. 11). It is striking to see that after the expansion of the authority to impose fines, the Dutch DPA has not used these more coercive deterrence instruments once during the entire timeframe of this research. Has the proverbial stick become too big, i.e. the impact of the fines so grave that they could hardly be imposed? The official document by the Dutch DPA continues on the subject by stating: *“With the expansion of the authority of the Dutch DPA to impose fines a transition towards the enforcement system under the future GDPR, which will replace the Dutch Data Protection Act, is realized”* (AP, *Boetebeleidsregels Autoriteit Persoonsgegevens* 2016, p. 11). The fines under the future GDPR, which will be enforced on the 25th of May 2018, will be expanded to a relative fine of four per cent of the annual worldwide revenue of a legal entity if an absolute fine of 20 million euro is deemed insufficient. In the collected documents no data was found directly related to the perception of the impact of the most coercive enforcement instruments under the Dutch Data Protection Act in the timespan of this research. There was one study found, ordered by Sophos and performed by Vanson Bourne, where the impact of the GDPR was assessed by interviewing 625 IT decision makers in the United Kingdom, France and the Benelux. One of the results was that: *“Almost one out of five (17 per cent) of the respondents admitted that they would have to close the business in case of a fine. This number rose to 54 per cent for smaller organisations with less than 50 employees. Closing businesses would not be the only effect: 39 per cent of the IT decision makers stated that the fines would also lead to having to fire people within their organisations”* (Sophos, 2017, para. 3).

Although the comparison with the situation under the Dutch Data Protection Act in the timespan of this thesis research is limited, the Vanson Bourne study shows that the impact of larger fines regarding the anticipated European privacy enforcement could result in the loss of business activities –provisioning of goods and services– and jobs.

Results ‘enforcement instruments’

In answer to question 5, the analysis shows that the kind of enforcement instruments available to the Dutch DPA have seen a significant change during the chosen timespan of this research. The most coercive –or deterring– instruments in its arsenal, being fines, have increased to a maximum of ten per cent of a legal entity’s annual revenue if 820.000 euro is deemed insufficient. Next to that, the fines are applicable to a significantly increased number of articles under the Dutch Data Protection Act

than before the 1st of January 2016. Despite these changes the Dutch DPA has, in the timespan of this research, from 2015 through 2016, not imposed a fine once.

The document analysis did not generate data that was sufficient to find an answer to question 6: it remains unclear whether the enforcement instruments available to the Dutch DPA affect its ability to perform its tasks, i.e. its ability to operate –by (de)escalation– an explicit enforcement pyramid. To conclude that the proverbial stick has been too small, an increase in the use of fines was expected after the 1st of January 2016 after expansion of the authority to use fines. Fact is that the Dutch DPA has not been using its ability to impose fines during the entire timeframe of this research. If the enforcement instruments were just right, they would not have seen enhancement after the 1st of January 2016. And from then on it remains a paradox why the enhanced instruments, i.e. the expanded fines, have not been used once. That the most punitive enforcement instruments, i.e. the imposable fines, might have turned into a stick being too big is only an indicative result of the study by Vanson Bourne (2017), which in comparison to this thesis research was conducted amongst a broader population regarding a future situation, where the proverbial stick will be even larger.

4.2.4 Level of discretion

Proposition ‘p4’ stating that the Dutch DPA operates with a level of discretion high enough to prevent it from escalation through the layers of the enforcement pyramid, raising issues of consistency of treatment across different regulatees –i.e. inequality and fairness– will be analysed for its likelihood in this paragraph. This proposition is derived from the seventh criticism, which states that high levels of discretion within the regulatory process can refrain regulators from escalating through the enforcement pyramid. The question to be answered is:

7. *Is there a level of discretion existent in the modus operandi of the Dutch DPA during the chosen timespan of this research?*

In an interview with the previous chairman of the Dutch DPA he states about the –at that time imminent– introduction of the obligation to report data leakages: *“The law does not force use to investigate all incoming reports. Of course we will pick a couple of whom we are suspicious”* (BNR, 2015, para. 7). Given this statement, it is clear that the Dutch DPA in 2015 was not obliged by law to respond, i.e. start escalating

though the enforcement pyramid, once an incoming report had come to its attention. This means there is a certain level of discretion the Dutch DPA can use. In the same article a reaction to the previous statement is provided on behest of a group of regulatees: *“Michael Steltman, director of the interest group Dutch Hosting Provider Association, states that the sector fears this will lead to arbitrariness [i.e. unwanted discretion] ... if companies will comply to the law they will on a precautionary basis report a lot to the Dutch DPA ... All these reports will have to be assessed ... Which will mean the Dutch DPA cannot process and further investigate all those reports and will pick out only those cases that will excite the public opinion. This will of course lead to arbitrariness”* (BNR, 2015, section *Willekeur*). We can infer from this that regulatees perceive an undesirable level of discretion used by the Dutch DPA to be existent, which in their opinion results in an arbitrary situation regarding the cases the Dutch DPA will act upon and which not.

In another article a less subjective form of discretion used by the Dutch DPA is emphasized: *“Under the GDPR consumers will be granted more rights to exercise more control over their personal information ... Next to this consumers can file a complaint at the Dutch DPA against an organisation. Under the GDPR the Dutch DPA is obliged to process the complaint of consumers. This could lead to a formal rejection of the complaint, but the Dutch DPA cannot ignore the complaints. Under the current law [i.e. the Dutch Data Protection Act] the Dutch DPA is not obliged to process complaints by consumers and consumers can only file a tip. Logically, under the GDPR, the Dutch DPA will have to act more as a result of complaints by consumers”* (Data Driven Marketing Association, 2017, section *‘Handhaving’ door consumenten*). This statement shows that regulatees, when comparing the level of discretion used by the Dutch DPA under the Dutch Data Protection Act to that under the anticipated European privacy law, understand that in the future situation the Dutch DPA is obliged to follow up on incoming reports by individual consumers. In the current situation –under the Dutch Data Protection Act– this is not the case and therefore the Dutch DPA is using a higher level of discretion, at least until the 28th of May 2018.

An article by the Dutch Platform for Civil Rights stipulates: *“Regarding several sensitive privacy dossiers the Dutch DPA remained unlawfully inactive, as concluded by Dutch courts this summer. This should be an incentive for the Dutch DPA to review its perception of its responsibilities to finally become an alert and critical*

privacy watchdog that protects the rights of civilians” (Platform Bescherming Burgerrechten, 2017, para. 1). This is the least subjective indication that the Dutch DPA is using a level of discretion due to the fact that it refers to Dutch court rulings which concluded that the Dutch DPA has remained unlawfully inactive in several enforcement cases (see www.zorgictzorgen.nl, *Autoriteit Persoonsgegevens verre van waaks als privacy-waakhond* [18th of May 2017]; www.privacybarometer.nl, *Rechter geeft Autoriteit Persoonsgegevens er van langs* [17th of July 2017]; www.computable.nl; *Rechter: AP reageert te laks op schendingen privacy* [19th of July 2017]; Rechtbank Midden-Nederland [2017] *AWB – 16 _ 3326 & AWB – 16 _ 4199*; Rechtbank Gelderland [2017] *AWB – 17 _ 2340*).

The analysis shows that at several occasions in the enforcement process the Dutch DPA acts at its own discretion. This can vary from more subjective forms, as perceived by regulatees in the case of the follow-up regarding the obligation to report data leakages, to more objective forms where Dutch courts had to intervene to demand enforcement in specific cases by the Dutch DPA. Overall it can be concluded that there is a level of discretion existent in the *modus operandi* of the Dutch DPA during the chosen timespan of this research.

This leads to the following question:

8. *How does the existent level of discretion used by the Dutch DPA affect its ability to perform its tasks?*

In the previously cited article by the Dutch Platform for Civil Rights the following passage articulates: *“The limited role of the Dutch DPA is frequently linked to the inadequate capacity of its organisation [i.e. the organisational resources], also by the Dutch DPA itself. And though the Dutch DPA is understaffed, this cannot be an explanation for the cases where she does use her capacity but does not persist”* (Platform Bescherming Burgerrechten, 2017, section *Smalle taakopvatting*). This shows that, next to the organisational resources, the level of discretion used by the Dutch DPA is perceived to be negatively affecting its ability to perform its tasks. The limited role of the Dutch DPA is illustrated by addressing the fact that there is no persistence in cases where the Dutch DPA does use its capacity. Further in the article its author continues: *“A lot depends on the decision the Dutch DPA is going to make*

regarding these dossiers. The choice comes down to persistence ... or to muddling through, which in fact would mean that the Dutch DPA is forsaking its responsibility as supervisor of a societal domain of which we just started to comprehend how big its influence will be on our daily lives. The Dutch DPA should adopt an assertive and leading role in this, instead of being overtaken by events or court verdicts” (Platform Bescherming Burgerrechten, 2017, section *Waak- of geleidehand?*). This quote reinforces the notion that the level of discretion used by the Dutch DPA is negatively affecting its ability to perform its task. It even goes so far as to state that in the cases where the Dutch DPA chooses not to persist it is forsaking its responsibility, which in extremis is eroding the reputation of the Dutch DPA as a regulator.

The analysis shows that the level of discretion the Dutch DPA uses in the enforcement process can lead to situations where it is not performing its task adequately, i.e. chooses not to escalate through the enforcement pyramid while it was entitled to do so. In the most concrete situations this is corrected by Dutch courts, which force the Dutch DPA to persist in her enforcement activities. These situations can lead to erosion of the reputation of the Dutch DPA as a regulator, which is a crucial element regarding successful regulation.

Results ‘level of discretion’

The answer to question 7 is that there is a level of discretion existent in the modus operandi of the Dutch DPA. Ranging from more subjective occasions to more objective occasions resulting in court cases, analysis has shown the level of discretion to be existent during the chosen timespan of this research.

The existent level of discretion in the modus operandi of the DPA, in answer to question 8, has negatively affected its ability to perform its task during the chosen timespan of this study. It can therefore be concluded that this existing level of discretion is high enough to prevent the Dutch DPA from escalating through the layers of the enforcement pyramid. The analysis has shown that in certain situations this has led to the perception –public opinion– that the Dutch DPA is unable to perform its task and to more objective court verdicts that indicate that in the involved cases the Dutch DPA has failed at its task, i.e. its ability to operate –by (de)escalation– an explicit enforcement pyramid. Regarding successful regulation and enforcement the influence of subjective perception in the public opinion should not be underestimated

as the theory (§2.1) states that failure to maintain reputation by regulators resides at the heart of enforcement failings (Baldwin et al., 2012).

4.2.5 Applicable law

This paragraph seeks to analyse the likelihood of proposition ‘p5’ stating that the Dutch DPA has to enforce a standard (the applicable privacy law), which is – perceived to be– vague, or susceptible to interpretation, preventing escalation through the enforcement pyramid. This proposition is derived from the fifth criticism, which states that the kind of standards imposed (and how these are received) is a factor influencing whether escalating through an enforcement pyramid is optimal. The question to be answered here is:

9. *What kind of standard –open or concrete–, i.e. applicable privacy law, does the Dutch DPA has to enforce during the chosen timespan of this research?*

An article discussing the –at that time– proposed expansion of the authority of the Dutch DPA to impose fines states: *“Vague norms and open concepts in the Dutch Data Protection Act need further substantiation. In a constitutional state fines can only be imposed when it is foreseeable in advance how to be compliant to the law”* (BirdBuzz, 2015, para. 1). This statement illustrates that the applicable privacy law in 2015, including its imminent expansion on the 1st of January 2016, was perceived to be consisting of vague norms and open concepts and depicts this as an undesirable situation within a constitutional state.

In another article the same statement is made: *“More frequently the security of personal information becomes the subject of legal requirements. Because legislation by definition is overtaken by events and technological developments are fast paced, laws are usually constructed in a ‘technology neutral’ manner. As a negative effect of this, rules become abstract and vague”* (ICTRecht, 2015, para. 1). This quote aligns with the previous citation by depicting the applicable privacy law in 2015, including its imminent expansion on the 1st of January 2016, as an open standard. It proceeds by providing an explanation for the Dutch Data Protection Act being an open standard, which is the result of intentionally keeping laws technology neutral in order to make them sustainable in the light of the fast paced technological developments.

In an interview the previous chairman of the Dutch DPA, Jacob Kohnstamm, states about the laws and regulations regarding privacy: *“We sometimes hear the critique that the law is too abstract. Legislative formulations should always be technology independent. You can’t continuously keep adapting the law to the technological developments. The expectation is that the granting of the expanded authority to impose fines will lead to more court cases against the Dutch DPA. This will lead to more jurisprudence and that’s what the law practice really needs. Jurisprudence will make the legislation more concrete, which will give organisations and consumers more guidance”* (Audit Magazine, 2016, [1], p. 9). This statement by the Dutch DPA’s previous chairman further reinforces the aforementioned quotes by depicting the applicable privacy law in 2015, including its imminent expansion on the 1st of January 2016, as an open standard. It also states that the Dutch Data Protection Act is an open standard as the result of intentionally keeping laws technology neutral in order to make them sustainable in the light of fast paced technological developments. The previous chairman of the Dutch DPA adds the element that he welcomes more jurisprudence, even as the result of court cases against the Dutch DPA, as it will create more clarity on how the applicable privacy law has to be interpreted.

In an interview regarding the protection of personal information by Dutch municipalities the vice chairman of the Dutch DPA, Wilbert Tomesen, is asked: *“Does the Dutch DPA wait too long before it starts enforcing? As supervisor the Dutch DPA could impose fines, right?”*. Tomesen replies: *“I sometimes feel the same frustration. You know: I want things to go right. If I start enforcing I might catch two or three municipalities. Leading to corrections at those instances. But I rather see the introduction of adequate additional legislation”* (NRC, 2016, para. 9). This answer of the vice chairman of the Dutch DPA reinforces the finding that during the chosen timespan of this research the applicable privacy law can be identified as an open standard.

The analysis shows that the kind of standard the Dutch DPA has to enforce during the period of 2015 through 2016, i.e. the Dutch Data Protection Act, can be qualified as an open standard (perceived to be vague or susceptible to interpretation).

The aforementioned leads to the next question:

10. How does the kind of standard, i.e. the applicable privacy law, the Dutch DPA has to enforce affect its ability to perform its tasks?

In the previously cited interview (Audit Magazine, 2016, [1], p. 9) a part of Jacob Kohnstamm statement regarding laws and regulations was: “ ... *The expectation is that the granting of the expanded authority to impose fines will lead to more court cases against the Dutch DPA. This will lead to more jurisprudence and that’s what the law practice really needs*”. This suggests that Kohnstamm expects an increase in enforcement cases, where the imposing of fines will –via jurisprudence– lead to a more concrete standard, i.e. applicable privacy law. As the analysis in paragraph 4.2.3 has shown, this increase in the imposing of fines has never been realized.

An article referring to the previously cited answer of Wilbert Tomesen, while discussing the protection of personal information by Dutch municipalities (NRC, 2016, para. 9), states: “*Actually the Dutch DPA is not very inclined to enforce, but rather awaits additional legislation. Every citizen in the Netherlands knows that legislation is a slow process*” (Zorg-ICT Zorgen, 2016, section *Krant*). This seems to be an indication that the kind of standard the Dutch DPA has to enforce is influencing the Dutch DPA’s ability to perform its task, i.e. its ability to operate an explicit enforcement pyramid. Where the previous chairman Kohnstamm wanted to solicit jurisprudence by more enforcement in order to achieve more clarity about the standard to enforce, the present vice president Tomesen –who also served under Kohnstamm– in a later interview suggests that he rather awaits additional legislation before he starts enforcing. This could explain why Kohnstamm’s strategy was never realized, although it remains speculative.

Due to the limited number of sources the relation between the kind of standard and the Dutch DPA’s ability to perform its task remains indicative.

Results ‘applicable law’

As an answer to question 9, the kind of standard the Dutch DPA had to enforce during the chosen timespan of this research can be identified as an open standard, which is perceived to be vague or susceptible to interpretation. This is most likely the result of the fact that laws are usually constructed in a technology neutral manner. Due to its

nature, the Dutch Data Protection Act applies for a significant part to situations where technology is a crucial aspect.

The answer to question 10 remains inconclusive. It seems that there is an indicative relation between the fact that the Dutch Data Protection Act can be qualified as an open standard and the fact that the Dutch DPA is –at times– reluctant to operate an explicit enforcement pyramid by escalation. Insufficient data was retrieved to prove a relation.

4.3 Results: likelihood of the propositions

This paragraph will provide an overview regarding the likelihood of the propositions, as analysed in §4.2.1 to §4.2.5, in the form of figure 11.

Proposition	Likelihood
The Dutch DPA does not need to escalate through the layers of the enforcement pyramid because the currently deployed enforcement instruments are sufficient to reach the adequate level of compliance. (p1)	<i>not likely</i>
The Dutch DPA lacks the resources –i.e. fte’s and budget– to be able to escalate through the layers of the enforcement pyramid. (p2)	<i>most likely</i>
The Dutch DPA lacks the right instruments –i.e. stick and impact too big or too small– to be able to escalate through the layers of the enforcement pyramid. (p3)	<i>inconclusive</i>
The Dutch DPA operates with a level of discretion high enough to prevent it from escalation through the layers of the enforcement pyramid, raising issues of consistency of treatment across different regulatees, i.e. inequality and fairness. (p4)	<i>likely</i>
The Dutch DPA has to enforce a standard (the applicable privacy law), which is –perceived to be– vague, or susceptible to interpretation, preventing escalation through the layers of the enforcement pyramid. (p5)	<i>inconclusive</i>

Figure 11. Likelihood of the propositions

5 Conclusion

5.1 Summary of analysis outcome

Figure 12 shows the summary of the analysis outcome. Proposition 1 has been rejected, propositions 2 and 4 have been accepted and propositions 3 and 5 are inconclusive.

Proposition	Result
The Dutch DPA does not need to escalate through the layers of the enforcement pyramid because the currently deployed enforcement instruments are sufficient to reach the adequate level of compliance. (p1)	<i>rejected</i>
The Dutch DPA lacks the resources –i.e. fte’s and budget– to be able to escalate through the layers of the enforcement pyramid. (p2)	<i>accepted</i>
The Dutch DPA lacks the right instruments –i.e. stick and impact too big or too small– to be able to escalate through the layers of the enforcement pyramid. (p3)	<i>inconclusive</i>
The Dutch DPA operates with a level of discretion high enough to prevent it from escalation through the layers of the enforcement pyramid, raising issues of consistency of treatment across different regulatees, i.e. inequality and fairness. (p4)	<i>accepted</i>
The Dutch DPA has to enforce a standard (the applicable privacy law), which is –perceived to be– vague, or susceptible to interpretation, preventing escalation through the layers of the enforcement pyramid. (p5)	<i>inconclusive</i>

Figure 12. Summarized analysis outcome

This leads to the situation in which we can answer the research question:

What factors determine the low level of coercion in the enforcement of Dutch privacy law by the Dutch Data Protection Authority during the period of 2015 through 2016?

Insufficient organisational resources of the Dutch DPA are the primary reason why there has been a low level of coercion in the enforcement of Dutch privacy law during the period of 2015 through 2016. The Dutch DPA lacked the number of employees and the annual budget to be able to operate an explicit enforcement pyramid to reach

an adequate level of compliance regarding the Dutch Data Protection Act during the chosen timespan of this research.

There is a level of discretion existent in the *modus operandi* of the Dutch DPA, which is high enough for it to be a secondary reason why there has been a low level of coercion in the enforcement of the Dutch privacy law during the timespan of this research. The analysis has shown that the level of discretion has been high enough to create certain situations during the period of 2015 through 2016 where it has led to cases in which the Dutch DPA did not escalate along the enforcement pyramid. The Dutch legal system had to intervene to correct the situations in which the Dutch DPA's reluctance to enforce was concluded to be unjustified and thus unlawful.

5.2 Reflection on results

The limitations of this research are the result of choices made by the author in light of practical issues. If the situation had allowed it, it would add to the societal and scientific relevance of this research to perform a multiple case study amongst different EU member state-DPAs. This would increase the generalizability of the results adding more value to the scientific discourse. The addition of interviews with relevant key figures amongst regulators and regulatees, if feasible, would increase the quality of the research design. It has to be mentioned that the drafting of propositions based on the theory was not exhaustive. More propositions could be drafted, but these were unlikely to be successfully operationalized using the present research design.

Another interesting element is the timeframe of the research. This was not a limitation, but it would be interesting to see what results are generated if in the future this research is repeated with the timeframe set to the period of 2019 through 2020. Compared to the current research the organisational resources of the Dutch DPA should have increased, the applicable law will be the GDPR and the enforcement instruments have been expanded once more. It can therefore be expected that the low levels of coercion, compliance and enforcement will be reduced, or might even have dissipated making it difficult to repeat this research. If not, it might be interesting to conduct the same research and compare the results.

Turning back to the research of this thesis, it can be stated that the results support the theoretical framework, which stipulates that a regulator should be able to operate an explicit enforcement pyramid to achieve compliance. The inability, or reluctance, to use the more coercive layers of its available enforcement pyramid has caused the

Dutch DPA's enforcement strategy to rely predominantly on a 'compliance' approach. This strategy contradicts the theoretical framework where it states that there should be a synergy or balance between 'compliance' and 'deterrence' approaches to achieve successful regulation (§2.2.2). Due to this imbalance the Dutch DPA has to a certain extent not been able to perform its tasks, which most likely explains why the level of compliance to Dutch privacy law over the period of this research has been low. This notion contributes to the academic –and societal– debate regarding persuasion versus punishment in regulatory systems: this research has shown that, to achieve successful regulation, both the carrot and the stick are essential. The debate should therefore, instead of focussing on intensifying or decreasing just one of them, focus on achieving more synergy –or balance– between the two.

To conclude, the results of this research show that in the Dutch case the deprivation of resources of the Data Protection Authority and the existence of a level of discretion in its modus operandi have led to situations where the protection of privacy rights has been at risk. Although the Dutch DPA by now has political consent for a significant expansion of its organisational resources, the question will be if the inevitable reformation of its organisation will be completed on time to effectively start enforcing the GDPR. And even though in every system driven by human decisions a certain level of discretion is existent, this level of discretion should not be high enough to lead to undesired outcomes in regulatory domains where the risks or negative consequences are high. In the case of regulatory systems, as theory has shown us, enforcement is about making highly complex trade-offs and balances in a way that is justified and the need for legitimacy runs through the entire regulatory process (Baldwin et al., 2012). To the author's opinion the regulation –and enforcement– of privacy law in the Netherlands deserves nothing less.

Abbreviations

AP	<i>Autoriteit Persoonsgegevens</i>
DPA	Data Protection Authority
DREAM	Detecting, Responding, Enforcing, Assessing and Modifying
EC	European Commission
e.g.	<i>exempli gratia</i> / for example
EU	European Union
fte	fulltime-equivalent
GDPR	General Data Protection Regulation
ICT	Information and Communication Technology
i.e.	<i>id est</i> / that is
N/A	not applicable
NOREA	<i>Nederlandse Orde van Register EDP-Auditors</i>
N/S	not specified
Wbp	<i>Wet bescherming persoonsgegevens</i>

References

- Andersson Elffers Felix. (2017). *Eindrapportage Organisatorische vertaling Verordening & Richtlijn Gegevensbescherming*. Retrieved from <https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2017/05/31/tk-bijlage-eindrapportage-aef-def/tk-bijlage-eindrapportage-aef-def.pdf>
- Allen & Overy. (2017). *The EU General Data Protection Regulation 2017*. Retrieved from <http://www.allenoverly.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf>
- Audit Magazine. (2016) [1]. *Bescherming van Persoonsgegevens begint aan de tekentafel*. Retrieved from https://www.iaa.nl/SiteFiles/AM/AM2016-01/Compleet_Audit_nr1_2016_def.pdf
- Autoriteit Persoonsgegevens. (2016). *1 jaar meldplicht datalekken: facts & figures 2016*. Retrieved from https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/factsheet_facts_figures_meldplicht_datalekken_2016.pdf
- Autoriteit Persoonsgegevens. (2016). *Bijlage jaarverslag 2015*. Retrieved from https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ap_bijlage_2015.pdf
- Autoriteit Persoonsgegevens. (2017). *Bijlage jaarverslag 2016*. Retrieved from https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ap_bijlage_2016.pdf
- Autoriteit Persoonsgegevens. (2016). *Boetebeleidsregels Autoriteit Persoonsgegevens 2016*. Retrieved from https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_van_de_autoriteit_persoonsgegevens_van_15_december_2015.pdf
- Autoriteit Persoonsgegevens. (2015). *De meldplicht datalekken in de Wet bescherming persoonsgegevens*. Retrieved from https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/richtsnoeren_meldplicht_datalekken_0.pdf

- Autoriteit Persoonsgegevens. (2016). *Jaarverslag 2015*. Retrieved from https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ap_jaarverslag_2015.pdf
- Autoriteit Persoonsgegevens. (2017). *Jaarverslag 2016*. Retrieved from https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ap_jaarverslag_2016.pdf
- Ayres, I., & Braithwaite, J. (1992). *Responsive Regulation: Transcending the Deregulation Debate*. Oxford: Oxford University Press.
- Baldwin, R., Cave, M., & Lodge, M. (2012). *Understanding Regulation: Theory, Strategy, and Practice*. Oxford: Oxford University Press.
- BirdBuzz. (2015). *Activistische CBP mag niet zomaar boetes opleggen*. Retrieved from <http://birdbuzz.nl/2015/02/04/activistisch-cbp-mag-niet-zomaar-boetes-opleggen/>
- Bits of Freedom. (2016). *Vier tips voor de nieuwe voorzitter van de Autoriteit Persoonsgegevens*. Retrieved from <https://www.bof.nl/2016/08/01/vier-tips-voor-de-nieuwe-voorzitter-van-de-autoriteit-persoonsgegevens/>
- BNR Nieuwsradio. (2015). *Autoriteit Persoonsgegevens komt straks handen te kort*. Retrieved from <https://www.bnr.nl/nieuws/10007311/autoriteit-persoonsgegevens-komt-straks-handen-tekort>
- Bowen, G.A. (2009). Document Analysis as a Qualitative Research Method. *Qualitative Research Journal*, (9)2, 27–40.
- Centric Netherlands. (2016). *Centric Security Survey 2016: Papieren Tijgers en Kippen Zonder Kop*. Gouda.
- Computable. (2017). *Rechter: AP reageert te laks op schendingen privacy*. Retrieved from <https://www.computable.nl/artikel/nieuws/overheid/6126118/250449/rechter-ap-reageert-laks-op-schending-privacy.html>
- Data Driven Marketing Association. (2017). *Privacy Monetization – over boetes en handhaving onder de AVG*. Retrieved from <https://ddma.nl/actueel/privacy-monetization-boetes-en-handhaving-avg/>
- Davidson, B., Hordern, V., Jackson, H., Lee, P., Levin, M., Pastor, N., Patrikios, A., Room, S., Sugard, S., & Taranto, L. (2012). *European Privacy: Law and Practice for Data Protection Professionals* (E. Ustaran, Ed.). Portsmouth, NH: International Association of Privacy Professionals.

- FinancieelDagblad.nl. (2017). *Miljoenenboete Facebook is kinderspel bij wat komen gaat*. Retrieved from <https://fd.nl/economie-politiek/1204827/miljoenenboete-facebook-is-kinderspel-bij-wat-komen-gaat>
- Gunningham, N., & Sinclair, D. (2017). *Regulatory Theory: Foundations and applications*. (P. Drahos, Ed.). Acton: ANU Press. 133–148.
- ICT Magazine. (2017). *De AP is geen showstopper voor innovatie*. Retrieved from <https://www.ictmagazine.nl/achter-het-nieuws/de-autoriteit-persoonsgegevens-is-geen-showstopper-voor-innovatie/>
- ICTRecht. (2015). *Wanneer is een beveiligingsniveau 'passend' volgens de wet?* Retrieved from <https://ictrecht.nl/2015/10/30/wanneer-is-beveiligingsniveau-passend-volgens-wet/>
- Jansen, M. (2017). *Wat het verleden ons kan vertellen over handhaving door de Autoriteit Persoonsgegevens*. Retrieved from <http://dirkzwageriteit.nl/2017/04/24/wat-het-verleden-ons-kan-leren-over-handhaving-door-de-autoriteit-persoonsgegevens/>
- Kluin, M.H.A. (2014). *Optic Compliance: Enforcement and Compliance in the Dutch Chemical Industry*. Ridderkerk.
- Makkai, T., & Braithwaite, J. (1993). The Limits of the Economic Analysis of Regulation: An Empirical Case and a Case for Empiricism. *Law and Policy*, 15(4), 271–291.
- May, P.J. (2007). Regulatory Regimes and Accountability. *Regulation & Governance*, 1(1), 8–26.
- Mendeloff, J. (1993). Overcoming Barriers to Better Regulation. *Law and Social Inquiry*, 18(4), 711–729.
- Ministerie van Veiligheid en Justitie. (2017). *Gevolgen Algemene verordening gegevensbescherming voor de Autoriteit Persoonsgegevens en meldingen datalekken*. Retrieved from <https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2017/05/31/tk-gevolgen-algemene-verordening-gegevensbescherming-voor-de-autoriteit-persoonsgegevens-en-meldingen-datalekken/tk-gevolgen-algemene-verordening-gegevensbescherming-voor-de-autoriteit-persoonsgegevens-en-meldingen-datalekken.pdf>
- Nederlands Tijdschrift voor Europees Recht. (2017) [6]. *Handhaving van de Algemene Verordening Gegevensbescherming vanuit Nederlands perspectief*.

- Retrieved from
https://www.recht.nl/exit.html?id=233048&url=https%3A%2F%2Fcms.law%2Fnl%2Fcontent%2Fdownload%2F313517%2F7916291%2Fversion%2F2%2Ffile%2FNtER_2017_06_b.pdf
- Nederlandse Orde van Register EDP-Auditors. (2015). *Privacy Impact Assessment: introductie, handreiking en vragenlijst versie 1.2*. Retrieved from
<https://www.norea.nl/download/?id=522>
- NRC Handelsblad. (2016). *De gemeente weet alles van je*. Retrieved from
<https://www.nrc.nl/nieuws/2016/04/19/de-gemeente-weet-alles-van-je-1612183-a845562>
- NRC Handelsblad. (2015). *Privacywaakhond CBP kampt met onderbezetting*. Retrieved from <https://www.nrc.nl/nieuws/2015/12/30/privacywaakhond-cbp-kampt-met-onderbezetting-a1410454>
- NU.nl. (2017). *Nieuw jasje voor Autoriteit Persoonsgegevens: 'De boetes komen'*. Retrieved from <https://www.nu.nl/weekend/4332953/nieuw-jasje-autoriteit-persoonsgegevens-de-boetes-komen.html>
- O'Leary, Z. (2004). *The Essential Guide to Doing Research*. London: Sage Publications.
- Platform Bescherming Burgerrechten. (2017). *Autoriteit Persoonsgegevens moet zich hoognodig bezinnen op haar rol*. Retrieved from
<https://platformburgerrechten.nl/2017/09/13/autoriteit-persoonsgegevens-moet-zich-hoognodig-bezinnen-op-haar-rol/>
- PricewaterhouseCoopers. (2017). *Privacy Governance onderzoek: Volwassenheid van privacybeheersing binnen Nederlandse organisaties*. Retrieved from
<https://www.pwc.nl/nl/assets/documents/pwc-privacy-governance-onderzoek-2017.pdf>
- Privacy Barometer. (2017). *Rechter geeft Autoriteit Persoonsgegevens er van langs*. Retrieved from
https://www.privacybarometer.nl/nieuws/3909/Rechter_geeft_Autoriteit_Persoonsgegevens_er_van_langs
- Rechtbank Gelderland. (2017). *AWB – 17 _ 2340*. Retrieved from
<https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBGEL:2017:3665>

- Rechtbank Midden-Nederland. (2017). *AWB – 16 _ 3326*. Retrieved from <https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBMNE:2017:3421>
- Rechtbank Midden-Nederland. (2017). *AWB – 16 _ 4199*. Retrieved from <https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBMNE:2017:3422>
- Security.nl. (2016). *Boetebedrag Autoriteit Persoonsgegevens naar 900.000 euro*. Retrieved from https://www.security.nl/posting/477371/Boetebedrag+Autoriteit+Persoonsgegevens+naar+900_000+euro
- Sophos. (2017). *Slechts een op de vier bedrijven in de Benelux begrijpt impact van de GDPR voor eigen organisatie*. Retrieved from <https://news.sophos.com/nl-nl/2017/06/16/slechts-een-op-vier-bedrijven-in-de-benelux-begrijpt-impact-van-gdpr-voor-eigen-organisatie/>
- Swire, P.P., & Ahmad, K. (2012). *Foundations of Information Privacy and Data Protection: A Survey of Global Concepts, Laws and Practices* (T. McQuay, Ed.). Portsmouth, NH: International Association of Privacy Professionals.
- Trouw. (2016). *Aleid Wolfsen Ombudsman van de privacy*. Retrieved from <https://www.trouw.nl/home/aleid-wolfsen-ombudsman-van-de-privacy~ab3660c6/>
- Van Rooij, B. (2006). *Regulating Land and Pollution in China. Lawmaking, Compliance, and Enforcement: Theory and Cases*. Leiden: Leiden University Press.
- Yin, R.K. (2014). *Case Study Research: Design and Methods* (5th ed.). Thousand Oaks, CA: Sage Publications.
- Zorg-ICT Zorgen. (2016). *Autoriteit Persoonsgegevens blaft, maar gaat ze ooit bijten?* Retrieved from <https://www.zorgictzorgen.nl/autoriteit-persoonsgegevens-blaft-gaat-ze-bijten/>
- Zorg-ICT Zorgen. (2017). *Autoriteit Persoonsgegevens verre van waaks als privacy-waakhond*. Retrieved from <https://www.zorgictzorgen.nl/autoriteit-persoonsgegevens-verre-waaks-als-privacy-waakhond/>