pro facto

Exploratory analysis

Public authorities' compliance with the AVG

Groningen, December 2022

www.pro-facto.nl

rijksuniversiteit groningen

Colofon

Pro Facto
Ossenmarkt 5
9712 NZ Groningen
www.pro-facto.nl
info@pro-facto.nl
050-3139853

Authors	Prof. Heinrich Winter, Bieuwe Geertsema, Thijs Drouen, Ernst van Bergen, Christian Boxum
Commissioned by	WODC
Date	December 2022
Status	Final report

This research was commissioned by the Dutch Scientific Research and Documentation Centre (WODC) and conducted by Pro Facto, an agency for administrative and legal research, consultancy and education.

The supervisory committee:
Prof. A.J.A. (Bert) Felling, Emeritus professor of methods, Radboud University (chairman)
Prof. L. (Leonie) Heres-van Rossum, Associate professor of local government integrity, Erasmus University, lecturer and researcher USBO, Utrecht University
Prof. E. (Elianne) van Steenbergen, associate professor of psychology of supervision, Utrecht University and senior supervisor behaviour & culture at the Financial Markets Authority
R. (Robbert) de Groot, senior policy officer, Ministry of Justice and Security
L. (Leontien) van der Knaap, project supervisor WODC

The researchers are responsible for the content of the report. Making a contribution (as an employee of an organisation or as a member of the supervisory committee) does not automatically mean that the contributor agrees with all the contents of the report. This also applies to the Ministry of Justice and Security and its Minister.

Summary

Background

Public authorities must comply with the standards of the General Data Protection Regulation (in Dutch: AVG) when processing personal data: the processing must be carried out in a way that is lawful, proper and transparent in relation to the data subject, be bound to specific purposes and not go beyond what is necessary for the purpose concerned. The data controller - the party who determines the purpose and means of data processing - must ensure that the data are accurate, implement appropriate organisational and technical measures for data security and be able to demonstrate that the data are processed with due care. The government has an exemplary role in complying with legal and treaty standards, and citizens must be able to trust that their data are properly protected. However, in recent years, there have been several instances where public authorities (both at the national and decentralised levels) have been found wanting in terms of AVG compliance. On 28 June 2021, it was agreed by the home minister and the legal affairs minister that an investigation should be conducted into public authorities' compliance with the AVG. This report describes the findings of this investigation.

Research question and topics

The objective of the research is to outline a picture of authorities' compliance with the AVG. The main research question reads as follows:

What are the most frequently encountered ambiguities and problems within government organisations in terms of AVG compliance and what causes can be identified?

To answer this question, we conducted an exploratory review of the current landscape of government compliance with the AVG, which was then further refined by means of nine case studies at different government organisations. Based on this exploratory review and the case studies, a new picture of authorities' compliance has been formed, on the basis of which a number of recommendations have been formulated.

Research methodology

In Chapter 2, we describe how one of the starting points of the study was to carry out more in-depth and broad-based research based on the existing picture of public authorities' compliance with the AVG. To this end, we started with a number of exploratory interviews with a view to gathering further information on the research topic. Subsequently, the research was carried out with the help of nine case studies at different government organisations: a government-level implementing organisation, a ministry, three independent administrative bodies (zbos), three municipalities and a water board. We selected an implementing organisation and zbos across different policy areas and of varying sizes. The same applies to the municipalities we selected, namely one of the four big cities, a 100,000+ municipality and a municipality with 35,000 inhabitants. As a decentralised, functional administrative body, we chose a medium-sized water board.

The first step in a case study is to conduct desktop research using available documents to form the best possible picture of how authorities manage their (privacy) organisation, the division of responsibilities and internal supervision. Interviews were then conducted with internal officers (all data protection officers (DPOs) and often (chief) privacy officers), other employees within the privacy organisation, employees or managers in the line organisation and someone from the board or management. At the end of the research, we presented and reflected on the findings and preliminary analysis with the experts in an expert meeting.

Legal framework

The AVG and the AVG Implementation Act (UAVG) provide the legal frameworks (Chapter 3) for this study. These regulate which roles are important when processing personal data and what the legal bases for processing personal data are. For public authorities, the relevant grounds are based on the necessity of data processing for 1) the fulfilment of a legal obligation incumbent on the relevant authority as a controller (Article 6(1)(c) of the AVG) or for 2) the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Article 6(1)(e) of the AVG). Within the legal framework, we then look at the requirements that apply to processing, the technical and organisational obligations that arise from it, and the tools available to the controller in this context.

Current picture

The first phase of the empirical research involved mapping the current picture of public authorities' compliance with the AVG (Chapter 4). To this end, we gathered information from the Association of Netherlands Municipalities (VNG), the National Audit Office (ADR), the Personal Data Authority (AP) and an independent expert who is contracted as an external DPO at several municipalities, plus some anecdotal findings from other publications.

It should be noted that the compliance picture for these interviewees is limited. Firstly, the picture of the AP (the regulator) is limited by the extent to which supervised authorities report alerts about data breaches. Also, only two employees are tasked with proactive, system-oriented supervision of the entire public sector on behalf of the regulator. The annually compiled 'sector picture' for the public sector could have been a valuable source for this study, but this is for internal information purposes only and has not been made available to us. The picture is also limited for the ADR and the VNG, being derived from audits and alerts that reach them within the scope of their advisory duties.

The impression conveyed by the interviewees is that municipalities do not always have sufficient knowledge of the relevant laws and regulations and how to apply them, while a lot of personal data is processed by the municipalities. The roles of data controller and processor are not always clear, and within the privacy organisation, there is often role confusion between the DPO and the privacy officer. The AP estimates that actvities such as DPIAs and securing responsibilities are not always well regulated and the independence of the DPO is regularly under threat. At the same time, there seems to be regular 'dominance of purpose', meaning that data processing is often seen as a solution to problems, without properly checking all the relevant boxes in the process. The overall picture is that compliance is developing positively. There is increasing awareness of the issue and this is being reflected in practice. With regard to departments and implementing organisations, the AP and the ADR note that there are strong differences in AVG compliance, sometimes per department and sometimes even per division. The ADR mainly sees a role for the organisational top; proper guidance is crucial for compliance across the organisation. In the AP's view, internal supervision can still be improved in a number of departments.

The ADR also notes that, in the past, DPOs were often expected to take on some of the responsibility for data protection. The ADR observes that departments always prioritise the primary process, with everything having to be done as quickly and efficiently as possible. Moreover, due to budget cuts, they often do not want to invest in privacy protection. Overall, however, developments in recent years have been positive, partly in response to the introduction of the AVG.

Findings from the case studies

Chapter 5 presents the condensed reports of the nine case studies. Chapter 6 lists the main similarities and differences.

Types of organisations
The type of administrative organisation can affect AVG compliance. Government organisations working with special personal data are more aware of the importance of the AVG and have always had a well-developed privacy organisation. In smaller organisations, privacy officers seem easily identifiable and approachable, while in large organisations there are greater opportunities when it comes to personnel to attract and retain qualified employees.

Policy and organisation
At all the organisations studied, we found that an up-to-date and complete privacy policy has been drawn up. At all the organisations, we observed some form of the three lines of defence model with the board as data controller (where this responsibility is mandated in the line organisation), supported by privacy officers (CPO and other privacy officers) and a DPO as advisor and supervisor. Also often positioned in the second line are the security officer and the chief information officer, who are responsible for information provision & digitisation policy and information systems management.

The situation in practice
In the case studies, we were unable to determine the exact level of compliance with the AVG in the specific actions of employees. At most, based on available documents and statements

from stakeholders, we were able to determine in a general sense the level of compliance and/or the direction in which it is developing.

We found that all organisations are devoting considerable attention to knowledge acquisition and the importance of attitude and behaviour. However, we do note that the level of knowledge varies between employees and is not always sufficient as of yet. One factor here is that data protection law is a complex area of law and answers to questions are not always easy to provide. Furthermore, time pressure and the dominance of policy goals have a disruptive role to play; we see this effect particularly strongly in the department and municipalities studied.

We observed that the boards and management of the organisations studied generally pay relatively high attention to the importance of compliance with the AVG, but that advice provided by the privacy organisation is sometimes ignored. To complicate matters further, questions and challenges relating to the AVG are often recognised late or not at all by front-line staff. The preparation of DPIAs is not always up to scratch; this is sometimes done too late and sometimes based on insufficient privacy expertise. Data breach protocols, however, are usually well established and well followed.

Issues

Besides the above mentioned issues regarding the dominance of policy goals and efficiency considerations, a second issue is the staffing of positions in the privacy organisation, partly due to the tight labour market. As a result, privacy officers are sometimes being pulled out of their roles because of a lack of knowledge or capacity elsewhere in the organisation. The third issue we identify is that compliance with the AVG is sometimes translated into a strong focus on technology and security, but less so on protecting personal data and safeguarding that interest in all processes within the organisation.

Conclusion

In the case studies, the prevailing picture is that focus on the proper processing of personal data has undergone a positive development following the introduction of the AVG, but is not yet at the desired level. The level of knowledge of the AVG among public authorities is increasing. But that does not mean that compliance with the AVG is necessarily always a matter of course. There is often no conscious decision in this regard. Sometimes there is a lack of sufficient awareness that an assessment of AVG considerations must precede any processing of personal data. Occasionally, there is an explicit choice not to comply, and the policy objective is leading at the expense of AVG compliance. In such cases, there is in fact a lack of willingness. But these are more the exceptions that confirm the rule that compliance with the AVG is improving.

Recommendations

The study leads to a number of recommendations aimed at strengthening AVG compliance within public sector organisations (chapter 7). We briefly present these recommendations here.

- We suggest that the Minister for Legal Protection and the Minister of the Interior and Kingdom Relations invest more in government organisations and that they adopt a stimulating role with a view to strengthening the privacy organisation at public sector organisations and embedding privacy awareness more strongly.
- Among public sector organisations, specific attention is needed for the timely inclusion of privacy concerns during the development of projects that will involve the processing

of personal data, for example through the timely preparation of a DPIA after a serious discussion of the relevant processes, risks and data ethics.

- The three lines of defence model is widely applied and is proving its worth. We do however see that filling key roles, including awareness officers in the line organisation, is difficult. This calls for targeted investments in existing staff, but also for commitment to the supply side of the labour market by encouraging training in this area.
- Organisations that involve a privacy officer and the DPO in the assessment and review process perform their responsibilities more substantively. A precondition for this is the presence of awareness officers, contacts or focal points in the first line. The case studies show that these officers are very valuable as ambassadors of the organisation's privacy policy. They can promote privacy awareness in the organisation and monitor how much relevance it has. For both management and the board, it is crucial to stress the importance of privacy protection, in word and in deed. This involves exemplary behaviour, but also the organisational safeguarding of privacy protection when weighing it against policy objectives. As a regulator, the AP seems to give priority mainly to the enforcement task.
- There is a clear need from the field for more communication, information and guidance from the AP. Specifically, it is desirable to facilitate more (informal) contact of a proactive and advisory nature. Where capacity problems in this area cause reticence, an expansion of that capacity might be the answer.
- The AP could opt for a broader interpretation of its duties in several areas. A greater effort to provide feedback to data breach reports would be beneficial. The AP's systemic supervision (currently only two staff) could also be reinforced, by investing in capacity and by deploying the existing network of DPOs more effectively.


pro facto