pro facto

Summary

# Data protected? Evaluation of the Dutch General Data Protection Regulation Implementing Act (UAVG), the duty to report data breaches and the power to impose fines

Groningen, June 22, 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 | Heinrich Winter, Thijs Drouen, Marlies van Eck, Lisanne Kramer, Bieuwe Geertsema, Jeanne Cazemier, Chantal Ridderbos-Hovingh |
| Commissioned by | WODC |
| Date | June 22, 2022 |

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 and Hooghiemstra & Partners, strategic and legal consultancy at the interface of data and law.

The supervisory committee:
Prof. Gerrit-Jan Zwenne (chairman; University of Leiden)
Dr. Jef Ausloos (UvA)
Paul Breitbarth (Catawiki)
Taetske van der Reijt (DWJZ, JenV)
Dr. Leontien van der Knaap (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.

**© 2022 Pro Facto. Copyrights reserved.**

# Summary

## Background

The General Data Protection Regulation Implementing Act (UAVG) entered into force on 25 May 2018. In accordance with Article 50 UAVG, within three years the Minister will send a report to the States General on the effects and the practical implementation of the UAVG. This evaluation consequently addresses both of these elements: how is the implementation proceeding and what are the effects of the law?

The UAVG and the General Data Protection Regulation (AVG) replace Directive 95/46/EC and the Personal Data Protection Act (Wbp). In the UAVG the Dutch legislator has chosen – where the regulation leaves room for national choices, or for a more detailed interpretation of rules – to build on the framework of standards from Directive 95/46/EC and the Personal Data Protection Act (Wbp). According to the explanatory memorandum, there was no time to develop a new framework. Another argument for minimising differences compared to the pre-AVG situation was the desire for a smooth transition from the old to the new situation.[1] The legislator therefore made provision for an evaluation (stipulated in Article 50 UAVG), the results of which can be used in a discussion about the need to amend the law. This is the scope of this evaluation.

Additionally, the research addresses the question of the extent to which the obligation to report data breaches is complied with and the extent to which the supervisory authority's power to impose fines contributes to an efficient and effective implementation and enforcement of the UAVG. On 1 January 2016 – while the AVG was about to be enacted – the Wbp was expanded to include the duty to report data breaches and the supervisory authority, from then on referred to as the Authority for the Protection of Personal Data (AP), was given the power to impose administrative fines. These components have been added to the evaluation in response to the 2015 motion by Members of Parliament Schouw and Segers requesting the government to evaluate the Dutch Data Breach Notification Act and the power to impose fines within four years of its entry into force.[2] The power to impose fines and the obligation to report data breaches were included in the AVG on 25 May 2016; the AVG applies from 25 May 2018.

[1] *Kamerstukken II,* 2017/18, 34851, no. 3, p. 4.
[2] *Kamerstukken II,* 2015/16, 33662, no. 20,

The UAVG is the organisational act that establishes the AP and lays down rules on its organisation (bodies, independence, etc.) and its tasks and powers. Otherwise, the UAVG follows the Wbp in respect of matters for which the AVG provides scope for the national legislature to make additions. It is important to note that the evaluation of the UAVG is emphatically not an evaluation of the AVG. Neither is it an evaluation of the AP. Insofar as the UAVG functions as an act establishing the AP, we have left these provisions out of consideration in our study. While this is an important starting point, it is unavoidable that the functioning of the UAVG will touch upon the AVG and that the effectiveness of administrative fines and the obligation to report data breaches will be influenced by how the AP exercises supervision and enforcement. In other words, it is unavoidable that our research will also touch upon the AVG and the AP.

This evaluation therefore covers:

— the working of the UAVG; and
— the compliance and effectiveness of the obligation to report data breaches and the application and effectiveness of administrative fines.

## Research questions

The overarching question central to the study is:

*How were the standards of the UAVG met in the period 2018 - 2020 and to what extent did the UAVG contribute to an efficient and effective implementation and enforcement of the AVG?*

The research was conducted on the basis of the following sixteen research questions.

1. How do lawyers, the AP and processors of personal data judge the clarity and accessibility of the UAVG?
2. To what extent are the standards of the UAVG clarified by the AP and case law?
3. What information is given to the different target groups at what time and in what way? What role does the AP play in this?
4. How do lawyers, the AP and processors of personal data judge the practicability of the UAVG?
5. How do lawyers, the AP and processors of personal data judge the enforceability of the UAVG?
6. How do processors of personal data comply with the provisions of the UAVG?
7. To what extent is the obligation to report data breaches complied with by processors of personal data?
8. What is the role of the Data Protection Officer within organisations, including in ensuring compliance with the reporting obligation?
9. To what extent does case law have a preventive effect with regard to compliance with the provisions of the UAVG and the obligation to report data breaches, and how could this be increased?
10. What is the supervisory strategy of the AP?
11. What is the enforcement policy of the AP?
12. How does supervision and enforcement by the AP take place in practice?

13. How is the seriousness of the breach of standards, the degree of culpability and an appropriate course of action determined when the AP exercises its power to impose fines?
14. To what extent does the authority to impose fines and the application thereof by the AP contribute to an efficient and effective implementation and enforcement of the AVG?
15. Is there any reason to change the AP's application of its powers and, if so, how?
16. How do lawyers, the AP and processors of personal data judge the extent to which the UAVG has exploited the scope that the AVG leaves for national choices in the implementation of the AVG?

## Method

**Fact-finding mission**

We started the study by gaining an orientation on the subject by studying relevant literature and documents, such as the legislative history of the UAVG, (legal) commentaries on the regulation, annual reports of the AP, the evaluation of the AVG by the European Commission of July 2020 and the consultation of the bill amending the UAVG.[3]

During this fact-finding mission, we also started the legal analysis and jurisprudence research that also served as input for the questionnaire survey and the other empirical research methods. In the first phase of the study, talks were held with (former) legislative lawyers and policy officers of the Ministry of Justice and Security with the UAVG in their portfolio, with some academic experts and with the chairman of the Dutch Association of Data Protection Officers (NGFG).[4]

In this phase of the study, we also wanted to have an informative discussion with the chairman of the board of the AP (Aleid Wolfsen). Due to objections raised by the Authority regarding the origins of the assignment, and the nature, set-up and scope of the research and the people involved, the AP decided, after several discussions between representatives of the ministry and the WODC and staff members of the AP, not to cooperate with the research at all. Later, however, we were able to submit a draft final text with questions. In response, the AP provided detailed comments and answers to questions asked. The researchers were able to benefit extensively from the AP's written response, which led to additions to the text in several places.

Following the refusal of the AP to cooperate with the research, the approach of the research was adjusted in consultation with the supervisory committee. This was done in two areas. As a result of the AP's refusal, the AP's Data Protection Officer register could not be used for the questionnaire survey of Data Protection Officers. The Privacy Law Association and the Dutch Association of Data Protection Officers (NGFG) were however willing to ask their members to participate in the digital survey. Neither could records of fines and notifications of data breaches at the AP be studied. For this reason, it was decided to carry out some case studies of decisions and notifications that have been publicised in the mainstream press. Otherwise, we discussed the application of the UAVG, the obligation to report data leaks and the power to impose fines with a large number of respondents.

**Legal analysis and caselaw study**

The legal sub-studies were given shape at the start of the project. In this way, the initial findings could also be used for the drafting of the questionnaire survey, on which the supervisory

[3] Annex 2 contains a list of the sources we consulted.
[4] A list of all the people interviewed during the evaluation is included in Annex 2.

committee provided comments, and the preparation of the topics to be discussed in the interviews. Within the framework of the legal sub-studies, interviews were held with various academic experts, lawyers specialising in data protection law and State Councillors of the Council of State.

**Questionnaire survey**
For the questionnaire survey, we wrote to a large number of data protection officers (an estimated two thousand who are members of the Privacy Law Association and the Dutch Association of Data Protection Officers (NGFG)), asking them to participate in the digital survey. In the end, we received responses from 190 data protection officers, working for administrative bodies (24%), social institutions (38%) and companies (37%). This spread of the respondents corresponds to the spread in the total population in our country.

**More in-depth interviews**
We conducted 33 in-depth interviews, including interviews with the management of a number of organisations (five), data protection officers (ten), lawyers (five), judges (three), some independent experts, such as academics (five) and (former) employees of ministries. We asked them about their views on how understandable the UAVG standards are and how applicable and enforceable they are.

**Case studies**
We conducted six case studies to form a picture, from start to finish, of a number of supervisory and enforcement processes involving the obligation to report data breaches and/or the instrument of an administrative fine. We studied a number of cases that have received publicity in the national press. Two cases were about the supervision and enforcement of a data breach: at Uber and the GGD GHOR. GGD GHOR Nederland is the umbrella organisation of the GGDs and GHOR agencies. GGD stands for Municipal or Community Health Service. GHOR stands for medical assistance organisation in the region. Three cases involved violations of other provisions of the AVG: Tax office/VAT number, Football TV and BKR (Financial Registration Office) Finally, research was carried out into the creation of the Code of Conduct for Health Care, given the importance of codes of conduct for the purpose of interpreting the open standards of the (U)AVG within sectors.

The findings and conclusions of the study are discussed below.

## General: the system

The AVG Implementation Act (UAVG) is a Dutch law that supplements the European General Data Protection Regulation. It is clear from the study that in fact the UAVG has only limited significance. In any case, it is clear that the law does not offer any more clarification of the AVG standards. This is perhaps understandable in view of the background to the UAVG, the limited time available for its creation and the choice made at the time for a 'policy-neutral' transposition of the existing standards. But that merely serves to limit the added value of the UAVG.

However, in the systematics of data protection law, in the combination of the AVG, UAVG and sectoral codes of conduct, it was precisely from those codes of conduct that an operationalisation of the standards in data protection law was expected. Against this background, the finding that codes of conduct have not been developed is important. Codes of conduct have the

potential to bolster compliance with the AVG standards by operationalising these in specific situations for a particular industry, or by providing options to choose between in a specific case. There are various reasons why more codes of conduct have not been developed, but one key reason seems to be the requirement for an independent and effective monitoring mechanism, which must be part of any code of conduct.

## How the UAVG works

**Clarity and accessibility**

The study shows that the clarity and accessibility of the UAVG are subject to criticism. The 'policy-neutral' interpretation of the law and the short time in which it had to be implemented were among the reasons for this. When examining to what extent the standards in the law have been further defined by the AP and in case law, the conclusion is that this has been done in part, but other parts still need further elaboration. Examples of this are given at various points in the research report. A clear example is the line taken by the Administrative Jurisdiction Division of the Council of State in its rulings of 1 April 2020 and 2 February 2022. In that case, the Division deemed itself competent to decide on a claim for compensation for damage arising from the processing of personal data pursuant to Article 8:88(1)(a) of the General Administrative Law Act (Awb) in conjunction with Article 34 of the UAVG. The survey conducted among data protection officers shows that they generally have a reasonable grasp of the standards. Bottlenecks do occur in some areas (such as the exceptions for processing special personal data and/or data of a criminal nature), but on the whole the data protection officers say they can work well with the standards.

**Practicability of the UAVG**

What has been said above about the clarity and accessibility of the UAVG has a direct relationship with the practicability of the UAVG. At various points, for example in chapter 6 of the report, comments are made on the provisions on automated decisions and on scientific research (see also section 7.2). In its supervision and enforcement, the AP focuses on the AVG, but also takes into account the standards of the UAVG. In the case studies, it emerged several times that parties under supervision need further clarification of the standards, and would like to discuss this with the AP. It appears from the case studies that the AP is not always prepared to conduct such a dialogue. On the other hand, the AP points out that prior to an intended processing operation, the AP can be asked for a so-called prior consultation, but so far little use has been made of this instrument. Also relevant to mention is that the AP says it regularly speaks with industry organisations (over 350 talks a year), in which a lot of attention is paid to the explanation of standards, including bankruptcies and the handling of transaction data by banks. The AP says it also has such discussions with legislative lawyers in ministries.

**Compliance with the UAVG**

The question regarding compliance with the provisions of the UAVG is difficult to answer. In general, the impression is that compliance with the AVG and UAVG is still an ongoing process of awareness-raising and implementation within organisations. Organisations are getting better at organising themselves with an eye to the risks involved in protecting personal data, but there is still room for improvement. The data protection officer plays an important role in many organisations when it comes to internal supervision of compliance with the provisions of data protection law. The majority of data protection officers say that they are involved in almost all data breaches in their organisation (60%). However, about one in six data protection officers think they are involved in less than half of the cases. The AP has set up a desk for

questions from data protection officers, where, according to the AP, around 100 questions a month have been received in recent years, which are also dealt with directly by the AP. From the questionnaire survey conducted among data protection officers, we see that most data protection officers serve as a contact point for the AP. But what is striking is that less than half of the respondents always feel free to approach the AP and a quarter never or only sometimes feel free to do so. It also emerges from the interviews that data protection officers are hampered by the fear that contact with the AP may lead to interventions or increased monitoring.

## Authority to impose fines and obligation to report data breaches

The research findings with regard to the power to impose fines and the obligation to report data breaches suggest that both instruments are useful in ensuring that the data protection law system functions properly when it comes to monitoring compliance. Nevertheless, this does not detract from the fact that in both cases there are also comments to be made about how the supervisory authority applies these instruments.

**Power to impose fines**

What is striking about the enforcement by the AP is that there is no policy rule setting out the supervision and enforcement policy. As far as we could ascertain, there is no known policy on this. So exactly how the AP operates with an escalation strategy is not clear. In the cases studied, there seemed to be little or no escalation strategy. It is also noteworthy that in a number of cases, a dialogue between the party under supervision and the AP was entirely or almost entirely absent. Even if the offender ceases the infringement, in the cases studied, the AP still imposes the fine. There is a policy on the mitigation of fines, but how this is applied in practice is not clear; in any case, a comparison of the cases did not provide any guidance on this point.

The adoption of supervisory and enforcement policies in which the administrative fine is accorded a place in the escalation model of the AP would create a great deal of clarity about how the AP operates. The expectation is that the parties under supervision will be more accepting of how they are treated by the AP. This is because the AP's behaviour would be more predictable and therefore more likely to be understood.

**Obligation to report data breaches**

The AP’s efforts to ensure compliance with the obligation to report are largely focused on data breaches that have been reported. Non-reporters seem to have more or less free play, although the AP itself states that it works with a risk analysis. In the case studies, we find that the AP imposes heavy fines precisely in cases where reporting has taken place. It is not inconceivable that this method of working will make potential reporters more reluctant to report. Timely reporting does not lead to a reduction of fines imposed for security deficiencies that come to light as a result of timely reported data breaches.


pro facto