FIDE report – Dutch Contribution Topic II

By Dominique Hagenauw and Hielke Hijmans (national rapporteurs), with contributions of Christiaan van Dissel, Sophie van der Hoeven-Bots, Violet Mantel, Olga Nijveld, Edmon Oude Elferink, Barbara Schenk, Merle Temme, Sybe de Vries and Martine Wijers.

A. Setting the Scene

Question 1:
The main national legal instrument introduced to implement the GDPR in the Netherlands is the GDPR Implementation Act (in Dutch: *Uitvoeringswet Algemene verordening gegevensbescherming* or *UAVG).* It was published in the Official Journal of the Kingdom of the Netherlands on 22 May 2018[1] and applies as of 25 May.[2] The Netherlands therefore completed their main legislative procedure for the GDPR just in time.[3]

The UAVG revokes the former Dutch personal data protection act (in Dutch: *Wet bescherming persoonsgegevens* or *Wbp*), it re-establishes the institution and powers of the Dutch supervisory authority, the Autoriteit Persoonsgegevens (hereinafter: AP),[4] and it supplements the GDPR by including certain derogations from the GDPR and by using so called opening clauses where the GDPR left some discretion to individual Member States.[5]

The GDPR Adaptation Bill (in Dutch: *Aanpassingswet Algemene verordening gegevensbescherming*, hereinafter: Adaptation Bill) - published in the Official Journal on 27 July 2018[6] - adapts existing references to the previous data protection legislation in a number of legislative acts in the Netherlands.

In implementing the GDPR, the Netherlands has refrained from making policy decisions where this would lead to a shift from the former data protection regime under the Wbp. Instead, the idea was to retain existing national standards and maintain the *status quo* as much as possible in order to enable a smooth transition from the old to the new regime.[7]

This approach is referred to as "policy-neutral", in line with the general approach in the Netherlands when implementing EU legislation.[8] Before making decisions to deviate from

[1] UAVG, https://www.officielebekendmakingen.nl/stb-2018-144.html, this link, just like all the others hereafter was last accessed on 19 June 2019. On the UAVG, see Hielke Hijmans, De AVG en de UAVG: Het grondrecht op gegevensbescherming wordt door de EU beschermd. De werking van dit recht in de Nederlandse rechtsorde roept vragen op, Nederlands Juristenblad 2018, afl 7.

[2] Royal Decree, https://www.officielebekendmakingen.nl/stb-2018-145.html.

[3] Paul Breitbarth, "The GDPR Implementation in the Netherlands", p. 1, https://blogdroiteuropeen.files.wordpress.com/2018/06/paul-1.pdf.

[4] Website AP, https://www.autoriteitpersoonsgegevens.nl/en/node/1930. See answers to questions 9-11.

[5] Articles allowing for the Member States to derogate are sometimes referred to as "opening clauses".

[6] Adaptation Bill, https://zoek.officielebekendmakingen.nl/stb-2018-247.html.

[7] EM UAVG, https://www.rijksoverheid.nl/documenten/kamerstukken/2017/12/13/memorie-van-toelichting-uitvoeringswet-algemene-verordening-gegevensbescherming.

[8] Paul Breitbarth, "The GDPR Implementation in the Netherlands", p. 4, https://blogdroiteuropeen.files.wordpress.com/2018/06/paul-1.pdf.

the *status quo,* the Dutch legislator intended to gain some experience with the GDPR for a number of years first.[9]

Existing national particularities, such as a stringent restriction on the use of social security numbers,[10] the treatment of data related to criminal behaviour as "special" personal data[11] and the minimum age for consent of 16,[12] have thus been retained. Especially the latter point, the age at which children can consent independently, is being debated extensively in the Netherlands. Currently, research is being done by the University of Leiden into the position of minors in the Netherlands civil procedure more generally, in view of possible legislative changes .[13]

Concerning the articles specifically mentioned in the question:[14]

- Article 6 GDPR, including article 6(1)(c) has not been separately implemented in the Netherlands. The reason given in the Explanatory Memorandum is that this article is no different than its predecessor in Directive 95/46/EG and the implementation thereof, the Wbp. The Explanatory Memorandum further explains that it can be expected that this legal basis will mostly be relevant for public authorities although it may also serve for the processing of data in the private sector. In this context, the obligation of banks to provide data about their clients to the Dutch tax authority (in Dutch: *Belastingdienst*) is mentioned as an example.[15]
- With regard to article 23 GDPR, this has been implemented in articles 41, 42 and 47 UAVG. The Explanatory Memorandum refers to this article as being complex and stresses the importance of the underlying ratio of article 23 GDPR; that the right to data protection can never be formulated in absolute terms, but must always be balanced against other rights and interests. It also points out that article 41 UAVG is merely the general provision and that sector-specific legislation may provide more guidance on how these exceptions are to be applied in a concrete case.[16]
    - Article 41 UAVG is almost exactly the same as article 23 GDPR, with one interesting deviation: the UAVG does not allow for the restriction of articles 22 and 5 GDPR. The Explanatory Memorandum states that, just like the Wbp, article 41 UAVG is subject to a strict necessity criterion, meaning that it does not provide a basis for structural and categorical restrictions of the rights of data subjects. Article 41 can only serve as a safety net in individual cases

[9] EM UAVG, https://www.rijksoverheid.nl/documenten/kamerstukken/2017/12/13/memorie-van-toelichting-uitvoeringswet-algemene-verordening-gegevensbescherming, last accessed 17 May 2019.

[10] UAVG, article 46.

[11] UAVG, article 31.

[12] UAVG, article 5(1).

[13] Letter of 1 April 2019 (32761, nr. 132), p. 12.

[14] EM UAVG, Implementation table (*Implementatietabel*), p. 70, https://www.rijksoverheid.nl/documenten/kamerstukken/2017/12/13/memorie-van-toelichting-uitvoeringswet-algemene-verordening-gegevensbescherming.

[15] EM UAVG, p. 29, https://www.rijksoverheid.nl/documenten/kamerstukken/2017/12/13/memorie-van-toelichting-uitvoeringswet-algemene-verordening-gegevensbescherming.

[16] EM UAVG, p. 40, https://www.rijksoverheid.nl/documenten/kamerstukken/2017/12/13/memorie-van-toelichting-uitvoeringswet-algemene-verordening-gegevensbescherming.

where it is necessary in that particular situation to restrict the applicability of the principles of data processing.[17]

- Article 42 UAVG provides that article 34 of the GDPR is not applicable to financial operators in the sense of the Financial Supervision Act (*Wet op het financieel toezicht* or *Wft*), because financial organisations within the scope of the Wft have a duty of care towards their customers and will have to notify them of faults or mistakes under that obligation.[18]
- Article 47 UAVG creates exceptions to the rights of data subjects with regard to public registers.[19] This article is based on a predecessor in the Wbp as well.[20] The Explanatory Memorandum specifies that the article is based on article 23(1)(e) GDPR. It also explains the specific function of public registries in order to clarify why it is so important that they are accurate and complete. As public registers have been set up by means of formal legislation, they have their own system to enable data subjects to access and change their data.[21]

- As mentioned above, the use of social security numbers has been under a strict regime before, and Article 46 UAVG stipulates that national identification numbers may only be used when explicitly provided for by law.[22]

The policy-neutral approach of the Dutch legislator has been subject to criticism. The Dutch parliament requested the government to make an inventory on a number of issues and take action where necessary.[23] Examples are the processing of data by smaller organizations (such as charities, sports associations, church communities and others), the processing of personal data at work in the event of sickness and the minimum consent age for children. In a letter of 1 April 2019[24] the minister for Legal Protection addressed and evaluated these concerns. Legislative steps to change the UAVG regarding some of these issues are being investigated.

Question 2:
Article 10 of the Constitution for the Kingdom of the Netherlands[25] contains the fundamental right to respect for one's private life (in Dutch: *persoonlijke levenssfeer*).[26] The article has been introduced in the Constitution in 1983. Article 10 of the Constitution also

[17] EM UAVG, p. 106, https://www.rijksoverheid.nl/documenten/kamerstukken/2017/12/13/memorie-van-toelichting-uitvoeringswet-algemene-verordening-gegevensbescherming.

[18] EM UAVG, p. 106, https://www.rijksoverheid.nl/documenten/kamerstukken/2017/12/13/memorie-van-toelichting-uitvoeringswet-algemene-verordening-gegevensbescherming.

[19] Article 21 GDPR (*Right to object*) is declared as generally not applying to public registers. Articles 15 GDPR (*Right of access by the data subject),* 16 GDPR (*Right to rectification*), 18 GDPR (*Right to restriction of processing*) and 19 (*Notification obligation regarding rectification or erasure of personal data or restriction of processing*) GDPR do not apply insofar as a special procedure has been established by law.

[20] EM UAVG, p. 112, https://www.rijksoverheid.nl/documenten/kamerstukken/2017/12/13/memorie-van-toelichting-uitvoeringswet-algemene-verordening-gegevensbescherming.

[21] EM UAVG, p. 112, https://www.rijksoverheid.nl/documenten/kamerstukken/2017/12/13/memorie-van-toelichting-uitvoeringswet-algemene-verordening-gegevensbescherming.

[22] In other cases article 46 UAVG also allows for deviation by general administrative order (*Algemene maatregel van Bestuur*) but also then no purpose for processing are acceptable which are incompatible with the original purpose for which the number has been processed (article 5(1)b GDPR).

[23] Motie Koopmans (34851, nr. 19) of 8 March 2018.

[24] 32761, nr. 132.

[25] Constitution of the Netherlands, https://zoek.officielebekendmakingen.nl/stb-2019-33.html.

[26] D.E. Bunschoten, commentaar op artikel 10 Grondwet, in: Tekst & Commentaar Grondwet en Statuut, Deventer: Kluwer 2018.

instructs the legislator to create rules protecting private life relating to the recording and provision of personal data, the rights to be informed, the right to have access to such data and to have it corrected.

The preamble of the UAVG, governing the protection of personal data, explicitly refers to article 10 of the Constitution.

Article 13 of the Constitution is also worth mentioning in relation to the protection of personal data, as it addresses the secrecy of correspondence, telephone and telegraph. An amendment aimed at broadening the scope of article 13 to "newer" kinds of communication has already been approved by both Chambers of the Dutch parliament.[27] For the amendment to come into force, the proposal to change the Constitution must be confirmed again by both Chambers after a general election has taken place.

A particularity of the Dutch Constitution is that no constitutional review of formal laws is possible. Article 120 of the Dutch Constitution provides that no judge will rule on the constitutionality of laws and treaties (in Dutch: *toetsingsverbod*).[28]

However, regulations of lower administrative bodies may be tested against the Constitution by the courts. Also, article 94 of the Dutch Constitution does allow for any law to be tested against any self-executing treaty. The ECHR is the treaty most commonly tested against by Dutch courts in this context.

Where appropriate, Dutch courts have in the past referred to Article 8 ECHR, because they could not directly invoke article 10 of the Constitution. In recent years, Dutch courts increasingly refer to articles 7 and 8 of the Charter.

In two Dutch cases where Article 8 of the Charter played a role, albeit in addition to article 8 ECHR.[29] Both were high-impact cases which eventually reached the Supreme Court of the Netherlands (in Dutch: *Hoge Raad*):

- An action by several individual citizens and an NGO (Privacy First) was brought against an amendment to the Passport Act, which obliged citizens to provide their fingerprints to be added to their travel documents. According to Privacy First, this requirement was contrary to Article 8 ECHR and Article 8 Charter.[30] Privacy First held that the creation of a central registry, the central storage (or not) of the data, the regime of providing data to others, the lack of necessary additional rules, the infringements on the principles of proportionality and subsidiarity and the amount of purposes for which the personal data would be stored, led to the new rules being unjustified. Eventually, the case was not resolved on the merits. The Supreme Court

[27] Proposal to change the Constitution, https://www.eerstekamer.nl/behandeling/20170914/publicatie_wet_2/document3/f=/vkhlc89peuxz.pdf.

[28] Nor does the Netherlands have a Constitutional Court.

[29] Cases which referred to article 7 of the Charter generally concern criminal law, immigration law and social security law-issues and are therefore not further elaborated on.

[30] ECLI:NL:HR:2015:1296, 22 May 2015, https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:HR:2015:1296.

dismissed the case in 2015 due to a lack of standing of both Privacy First and the individuals concerned.

- The association of practicing General Practitioners (GPs) brought a case against a newly established system allowing for the (far-reaching) electronic processing of medical personal data in the Netherlands.[31] The system would allow primarily for GPs[32] to access personal data of a patient, in addition to a "professional summary" created on the basis of the GP's own patient file. This system, according to the association, unnecessarily infringed upon patients' rights to privacy, specifically article 10 of the Dutch Constitution, article 8 ECHR and article 8 Charter.[33] The *Hoge Raad* however agreed with previous instances that the proportionality and subsidiarity was sufficiently respected.

Both cases were decided before the GDPR came into effect, which means that it cannot be said with certainty that future cases invoking article 8 of the Charter will be assessed similarly by Dutch courts.

Question 3:
In the Netherlands the interpretation of the principles of fair processing, purpose limitation and data minimisation varies strongly per sector, hence no 'one true answer' can be given for their application.

In June 2018, the AP has looked into the processing by the Netherlands Tax and Customs Administration of the national identification number (BSN) in the VAT-identification numbers of freelancers.[34] The AP states in its final report that by converting the BSN and using it as (part of the) VAT-identification number, the BSN is used improperly as this would result in essence that a person is forced to reveal his or her BSN publicly and to third parties, in violation of the UAVG and the principles of fair and lawful processing of article 5(1)(a) of the GDPR. The Dutch Tax and Customs Administration is required to take measures to address the situation before 1 January 2020.

Another interesting example concerns the Dutch system of credit registration. Credit providers are obliged to take part in a system of credit registration and need to register credits above € 250. Whenever a debtor doesn't commit to paying instalments, that person gets a 'negative registration' in the system. The information in the system can be used by new credit providers to determine whether the consumer has a financial situation (un)suitable for a newly requested credit. There are a myriad of court cases against the credit providers registering a consumer in the system concerning their negative registrations, which consumers become aware of when learning that they are not eligible for new credits and mortgages as a result of these negative registrations.

[31] ECLI:NL:HR:2017:3053, 1 December 2017, https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:HR:2017:3053.

[32] Thus GPs who are temporarily filling in for the patient's own GP.

[33] Another main complaint brought forward by the association was that the system relied on consent of the patient as a legal basis for processing (as opposed to an obligation established by law) and could, on that ground, not provide a basis for infringing medical confidentiality. It is worth noting that a legal proposal which intended to create a proper legal framework for such as system had been rejected by the Dutch Senate in 2011.

[34] "Onderzoek naar de verwerking van BSN in btw-identificatienummers door de Belastingdienst", Autoriteit Persoonsgegevens, June 2018.

In 2011, the Dutch Supreme Court ruled that the registration should at all times be in accordance with the principles of proportionality and subsidiarity.[35] It further held that under certain circumstances it may not be the negative registration itself, but the minimum registration period of five years, that is disproportionate with regard to the purpose of the processing of the data, which is combating over-crediting consumers and protecting credit providers from financial risks.

Question 4:
Similar to the answer to question 3, there is no 'one true answer' for the use of the legal grounds of legitimate interest and consent. There are nevertheless interesting cases to be mentioned.

First of all, a recent ruling from a local court reaffirms the use – under certain conditions - of the legal ground of legitimate interest for processing personal data by using security cameras.[36] In the case at hand, the security camera was only recording a small part of a public road and people walking there would not be recorded fully. The owner of the camera demonstrated that less-intrusive security means were not sufficient to protect his property and the people and goods on it. Recording of images was needed to support any filing to the police. Moreover, people were informed that a security camera was recording images and the owner of the security camera had verified its compliance with necessary safeguards. These reasons led the Court to rule that the "legitimate interest" could be used in this case.

With regard to the legal ground of consent, a relevant court case is on the national linking point for patient data (LSP).[37] Following concerns of doctors, a case went up to the Supreme Court on whether the consent of a patient who needs medical attention would be sufficient to allow access to his or her medical record in case the doctor who had received the consent and kept the record was not available. The Supreme Court upholds judgements of the lower courts in affirming that the patient's consent did sufficiently meet the requirements of freely given, specific and informed sufficiently and could therefore be relied upon for accessing and processing personal data of patients in absence of their "regular" doctor.

Question 5:
In the Netherlands the debate on the validity of personal data as a counter-performance for the provision of digital content is not only related to the GDPR, but also to consumer law, especially the Digital Content Directive.

Even though there is no clear indication that public debate in the Netherlands mostly opposes to the use of personal data as counter-performance *per se,* both Chambers of the Dutch Parliament have put questions to the government concerning the lack of clear coordination between the Directive and the GDPR.[38]

---

[35] HR 9 September 2011, NJ 2011/595.

[36] https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBMNE:2019:2725

[37] https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:HR:2017:3053&showbutton=true&keyword=ECLI%3aNL%3aHR%3a2017%3a3053

[38] file:///Users/gebruiker/Downloads/beantwoording-aanvullende-kamervragen-over-richtlijnvoorstel-levering-digitale-inhoud-en-diensten.pdf

The discussion *inter alia* revolved around which would be the correct lawful basis for processing personal data to deliver digital content, mainly focusing on whether this can only be the consent of person concerned or whether also other legal grounds would be possible.

Another important question that was raised is whether personal data in case of terminating the agreement should be valued in money and whether the consumer as a consequence should be financially compensated. The Dutch government, without further explanation, simply states that this is not necessary. The organization should either return the personal data to the consumer, or, if this is not possible, pay money as a form of compensation. The problem observed in legal literature is whether industry can be burdened with potentially millions of euros in collective actions initiated by consumers.[39]

Question 6:
Article 40 UAVG provides for exemptions from the prohibition on automated individual decision making. These exemptions however take into account that not all cases of automated decision making pose high risks in terms of a potential discriminatory effect. For example, automated individual decision-making regarding 'closed' decisions, that are based on the fulfillment of objective requirements, do not inhibit a high risk. Think of processing income data for taxation purposes or basing traffic fines on photographs in combination with license plates.

In addition, the article provides for several safeguards. First, a controller can only apply these exemptions for processing based on article 6(1)(c) or (e) GDPR.[40] Furthermore, the controller needs to take adequate measures for the protection of personal data. For controllers that are not administrative bodies, such appropriate measures shall have been taken if the right to human intervention, the data subject's right to express his or her views and the right to contest the decision, are safeguarded.

However, and provided other adequate measures are being taken by the controller to safeguard the data subject's rights, freedoms and legitimate interests, the requirement of human intervention may be set aside.

For automated decision making by a government institution, the General Administrative Law Act (in Dutch: *Algemene wet bestuursrecht* or *Awb*) is applicable, in addition to the GDPR. This general law provides for comparable safeguards and principles that must be taken into account in decision making, including the principles of diligence and proportionality. It also provides for a subject's right to appeal decisions.

However, in its letter to the House of Representatives of April 2019 regarding the first experiences with the UAVG [41] the government responded to the request of the Dutch Trade Association[42], to create a more generous exemption to offer more options for innovation

[39] Schulte-Nölke (2018), p. 75.

[40] Processing necessary for compliance with a legal obligation to which the controller is subject or processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

[41] TK 2018/19, 32 761, nr. 132.

[42] VNO-NCW and MKB Nederland

regarding new profiling-based techniques. The government indicated in the aforementioned letter to uphold its decision not to include an exemption in the UAVG for automated decision making using profiling-techniques. It held that the risk that group-characteristics are attributed to an individual whilst it is not 100% certain that this individual, although belonging to the group, also has those specific characteristics, in combination with automated decision making, is considered too great a risk.

The government has furthermore informed The House of Representatives that a working group is creating guidelines for the transparency of algorithms used by the government as well as guidelines for the information of the public about big data applications of the government. The government is also looking into the possibility to create extra legal safeguards for big data applications by the government.[43]

Question 7:
After the *Google Spain and Google* ruling[44], Google immediately put in place a search removal form on its website and made available a Transparency Report.[45] Between May 2014 until May 2019, somewhat over 150.000 requests for delisting URLs were made by users in the Netherlands. Out of this total 49,4% of requests were granted (about 3% higher than EU average). After 25 May 2018, the percentage of URLs that were delisted increased from 47,8% to 56,3%, an increase of almost 10%. This may be explained by the strong awareness campaign for privacy led by the AP and the government in the months prior to this date.

Consumers may also, instead of addressing search engines directly, turn towards the AP to act as an intermediary. The AP uses the guidelines of the Working Party 29 as well as conditions derived from national and EU case law to determine whether the listing of the URL after a search inquiry is justified. However, only 5% of all incoming complaints were requests for intermediary action.[46]

Between 2014 and July 2019, 24 cases can be found where the right to be forgotten was invoked before a Dutch court. Only in six of the 24 cases did the judge rule in favour of the plaintiff.

Question 8:
Article 85 of the GDPR was implemented in relation to journalistic purposes and for academic, artistic and literary expressions in article 43 UAVG. Given the 'policy neutral' implementation of the GDPR in the UAVG, most of the exemptions that were already created in the Wbp still apply. [47] This means that the majority of articles of the GDPR do not apply to the processing of personal data solely for journalistic purposes and for the purposes of academic, artistic or literary expression, including articles 9 and 10 of the GDPR

[43] TK 2018/19, 26 643, nr. 601

[44] Case C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (es), Mario Costeja González, ECLI:EU:C:2014:317, 13 May 2014..

[45] Transparency Report "*Search removals under European privacy lawi*", Google.

[46] "Klachtenrapportage: facts & figures. Overzicht 25 mei tot 25 november 2018", Autoriteit Persoonsgegevens.

[47] Articles 7(3) and 11(2), Chapter III, Chapter IV (with the exception of Articles 24, 25, 28, 29 and 32), Chapter V, Chapter VI and Chapter VII of the GDPR.

concerning the prohibition to process special categories of data or data relating to a criminal convictions and offences.

The fact that not all provisions of the GDPR are applicable to data processing for journalistic purposes or for the purposes of academic, artistic or literary expression, does not mean that the privacy of the subjects is not being weighed. First, the general provisions and basic principles of the GDPR are still applicable. Second, a balancing of the right of freedom of expression and the right to privacy in concrete cases will be executed by the court, with account to the specific circumstances of the case.[48]

Furthermore, some new elements have been introduced to keep in line with jurisprudence, like the exemption to the right of the data subject to withdraw his or her consent at any time.[49] This would mean for example that, once permission has been given for publication of an interview, this can generally not be withdrawn.

The Board of Journalism (in Dutch: *Raad voor de Journalistiek*) and the Dutch Society of Journalists (in Dutch: *Nederlandse Vereniging van Journalisten*) both have a code of conduct. These contain guidelines on the proportionality of interferences with privacy for journalistic purposes.

Lastly, in its letter to the House of Representatives regarding the first experiences under the UAVG the government stated that it will not follow the *NDP Nieuwsmedia's* (a trade organization for news companies), stance that more provisions of the GDPR should be exempted.[50] The government considers the current provisions necessary for a proper balance between the protection of privacy on the one hand and the freedom of expression on the other hand.

Question 9:
The AP is established as the sole data protection supervisory authority of the Netherlands).[51] According to Dutch public law, the AP is an autonomous administrative authority (in Dutch: *zelfstandig bestuursorgaan* or *ZBO*) at the level of the central government; it is endowed with legal personality.[52] In the Netherlands, autonomous administrative authorities are authorities that have been vested with public authority, but do not hierarchically subordinate to a minister. These authorities are created for instance where strict regulations have to be applied in large numbers of many individual cases, where independent experts have to be called in to carry out quality checks, issue licenses or grants, or where independent experts have to monitor the implementation of regulations.[53]

General provisions on autonomous administrative authorities are included in the Autonomous Administrative Authorities Framework Act (in Dutch: *Kaderwet ZBO's*). This act

[48] De pers en privacy. Hoe verhoudt de AVG zich tot het juridisch kader voor de journalistiek? Noot bij Rechtbank Amsterdam, 12 oktober 2018, ECLI:NL:RBAMS:2018:7397 (Oudkerk/Sanoma).

[49] An exemption to article 7(3) of the GDPR.

[50] TK 2018/19, 32 761, nr. 132.

[51] Article 6(1) of the Implementation Act.

[52] Article 6(1) of the Implementation Act.

[53] See also: <https://www.overheid.nl/english/about-the-dutch-government/what-government-consists-of/autonomous-administrative-authorities>, visited 1 August 2019.

creates a legal framework that deals with the responsibilities of the minister on the one hand and the administrative body on the other hand.[54] The minister responsible has a limited number of powers, like the power to approve the budget.[55] These matters are specified when a ZBO is set up. The minister is only responsible for using these powers and not for the decisions made by the ZBO itself.

The minister responsible for the AP is the Minister for Legal Protection. In order to fully guarantee the independence of the AP, certain sections of the Framework Act do not apply to the AP. As a consequence, the Minister for Legal Protection does, inter alia, not have the power to lay down policy rules relating to the way in which the AP performs its tasks[56] and to annul decisions of the AP.[57]

Composition; appointment process for members and staff
The AP comprises of a Chair and two other members.[58] The Chair, who shall satisfy the requirements for appointment as a judge, and the other members of the AP are appointed by royal decree on the nomination of the Minister for Legal Protection.[59] The term of office for chairman and members of the AP is 5 years.[60] They can once be re-appointed for a term of another 5 years.[61] The AP has a Secretariat whose officials are appointed, promoted, disciplined, suspended and dismissed by the AP.[62]

Powers and duties
The Awb regulates the process of administrative decision-making in a general sense and provides a general framework for the right of appeal to an administrative court against the orders issued.[63] Chapter 5 of the Awb relates to administrative enforcement action by administrative authorities, including general rules for monitoring compliance by inspectors and for administrative sanctions. As a result, at a national level, both the Awb and the UAVG deal with powers of the AP.

Under the UAVG, the AP is competent to perform the tasks and exercise the powers that are conferred on supervisory authorities by or pursuant to the GDPR.[64] the members and the officials of the AP, as well as other persons designated by the AP, are responsible for monitoring compliance with the GDPR and with other relevant legislative provisions.[65] As a result, the **investigative powers** with which 'inspectors' are empowered according to

[54] See also Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Evaluatie Kaderwet zelfstandige bestuursorganen 2012-2016, May 2018.
[55] Cf. Chapter 4, Division 1, of the Autonomous Administrative Authorities Framework Act. See also: <https://www.overheid.nl/english/about-the-dutch-government/what-government-consists-of/autonomous-administrative-authorities>, visited 1 August 2019.
[56] Article 13(1) of the Implementation Act.
[57] Article 13(1) of the Implementation Act.
[58] Article 7(1) of the Implementation Act.
[59] Article 7(3) of the Implementation Act.
[60] Article 7(5) of the Implementation Act.
[61] Article 7(6) of the Implementation Act.
[62] Article 10(1) of the Implementation Act.
[63] See also: T. Barkhuysen, W. den Ouden and Y E. Schuurmans, 'The Law on Administrative Procedures in the Netherlands', NALL 2012, april-juni, DOI:10.5553/NALL/.000005.
[64] Article 14(1) of the Implementation Act.
[65] Article 15(1) of the Implementation Act.

Chapter 5 of the Awb are also entrusted to the AP.[66]

The investigative powers granted to supervisory authorities by the GDPR closely resemble the investigative powers mentioned in the Awb. In some cases, the Awb seems to be more wide-ranging, for instance when it comes to the subject of the investigation. The Awb states that "everyone" shall be obliged to cooperate fully with a supervisor[67], whilst Article 31 of the GDPR stipulates only that the controller and the processor (or their representative) should cooperate with the authority. There seems to be no legal obstacle to combine the investigative powers granted by the Awb and the GDPR.[68]

In addition to the **enforcement powers** provided by the GDPR, the AP has extra enforcement powers pursuant to article 58(6) GDPR, in particular administrative enforcement orders, either under the threat of enforcement action by or on behalf of the AP itself (in Dutch: *last onder bestuursdwang*) or under periodic penalty payment (in Dutch: *last onder dwangsom*). The power to impose these orders is derived from the Awb.[69] With such an administrative order, the AP can for example order a controller to comply with the GDPR and the UAVG. If the controller fails to comply with the order within the prescribed time limit, a specified amount of money must be paid. Furthermore, the AP can order any company or person to cooperate with the AP.[70]

The UAVG also provides that the administrative fines of article 83 GDPR may be imposed on *public* authorities and bodies, using the option given in article 83(7) GDPR.[71]

Lastly, the Implementation Act provides the AP with the power to **mediate**. The interested party may file a request with the AP to mediate in or advise on his or her dispute with the controller in cases concerning articles 15-22 of the GDPR.[72] In 2018, the AP has mediated in 129 cases.[73] These cases mainly concerned requests to delist search results on a person's name in a search engine (see also question 7). In most cases the search results were delisted after mediation by the AP.

The AP is not only responsible for monitoring compliance with the GDPR and the UAVG, , but also ensures compliance with – among others – the Elections Act (in Dutch: *Kieswet*), the Basic Registration of Persons Act (in Dutch: *Wet basisregistratie personen*) and the Dutch Acts implementing Directive (EU) 2016/680: the Police Data Act (in Dutch: *Wet politiegegevens*) and the Judicial Data and Criminal Records Act (in Dutch: *Wet justitiële en strafvorderlijke gegevens).*

[66] See also: V.N. Mantel, E.S. van der Deijl and E. Los, 'De (U)AVG en de Awb: toezicht, sanctionering en rechtsbescherming', **JBplus** 2019/01.

[67] Article 5:20 of the Awb.

[68] See also: V.N. Mantel, E.S. van der Deijl and E. Los, 'De (U)AVG en de Awb: toezicht, sanctionering en rechtsbescherming', **JBplus** 2019/01.

[69] Article 16(1) of the Implementation Act and articles 5:21 and 5:32 of the Awb.

[70] Article 16(2) of the Implementation Act

[71] Article 18(1) of the Implementation Act in conjunction with Article 83(7) GDPR.

[72] Article 36(1) of the Implementation Act.

[73] Annual Report 2018, <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ap_bijlage_2018.pdf>, visited 2 August 2019.

Question 10:
The starting point for complaint handling is that the AP will investigate the subject matter of complaints to the extent appropriate.[74] The AP has published policy guidelines on how it will prioritize the handling of complaints lodged with it under the GDPR (*Beleidsregels prioritering klachtenonderzoek AP*).[75] According to these guidelines, the AP will **firstly** determine whether the complaint concerns the processing of personal data relating to the complainant[76], and whether basic desk research leads to the conclusion that there is a clear violation of the GDPR – or to the conclusion that it is clear there is no breach of the GDPR, in which case the complaint will be rejected.

As a general rule, according to Dutch administrative law, the AP is required to take legal action (by means of a reparatory sanction) when it establishes an infringement of the GDPR after receiving a complaint in writing, lodged by an interested party, aimed at enforcing compliance with data protection rules.[77]

However, if the AP is able to resolve a complaint successfully by – for instance – offering guidance to the controller (thus taking 'informal enforcement action'), after which the controller brings its processing into compliance and the complainant is satisfied, the AP will close the case.

If the desk research points out that an infringement of the GDPR might occur, but a more thorough investigation is necessary in order to come to more definitive conclusions, the AP will **secondly** determine whether there is reason for further investigation. Criteria include:

a. How harmful is the alleged violation for the individual(s)?
   This depends on nature of the personal data involved and on the nature of the alleged violation.
b. What is the broader social significance of the case, taking into account the areas of special focus the AP publishes on a regular basis?
   The AP issues focal areas for the coming year,[78] and takes into account the number of individuals concerned and whether or not the complaint concerns cross-border processing.
c. To what extent will the AP be able to act effectively?
   The AP will take into consideration other complaints filed with the AP, its available manpower and budget.

In 2016, the Administrative Jurisdiction Division of the Council of State, ruled that the pre-GDPR guidelines on complaint handling did not violate Directive 95/46/EC.[79] The Council of

[74] Article 57(1)(f) of the GDPR. See also O.S. Nijveld and W. van Steenbergen, 'Het Awb-landschap door een AVG-filter', **TvT** 2018-4, p. 95-102.
[75] *Stcrt.* 2018, 54287.
[76] Also a not-for-profit body, organisation or association that is active in the field of the protection of data subjects' rights and freedoms and can be considered an 'interested party' in terms of Article 1:2(3) of the Awb, independently of a data subject's mandate, has the right to lodge a complaint with the AP.
[77] ABRvS 11 August 2004, *AB* 2004, 444 (m.nt. F.R. Vermeer).
[78] See the Supervisory framework, <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/toezichtkader_autoriteit_persoonsgegevens_2018-2019.pdf>, visited 2 August 2019.
[79] ABRvS 19 October 2016, ECLI:NL:RVS:2016:2743.

State found that the guidelines did not form a violation of the obligation to guarantee the application and effectiveness of EU law.

Question 11:
Besides sanctions and corrective measures as referred to in article 58(2) GDPR and additional sanctions adopted at national level[80], the AP also uses 'informal' enforcement instruments to obtain compliance (for instance, in reaction to a complaint[81]). Examples may include meeting with a controller to offer guidance on a specific GDPR provision violated (in Dutch: *"normoverdragend gesprek*") or issuing a guidance letter (offering guidance on compliance with the requirements of the GDPR).[82]

GDPR sanctions and additional sanctions
In 2018, the AP took enforcement actions against 17 private companies, public authorities and other organisations. The AP imposed sanctions in six cases, four of which are published:

- The AP imposed an administrative fine pursuant to Article 83 GDPR on Uber B.V. and Uber Technologies, Inc. of €600,000 for violating the data breach regulations.[83]
- The AP imposed a ban on processing as referred to in Article 58(2)(f) GDPR against the Netherlands Tax and Customs Administration which may no longer process the national identification number as part of the VAT number of self-employed persons (see further answer 3).[84]
- The AP imposed an administrative enforcement order under periodic penalty payment[85] – an additional sanction adopted at national level – against the Employee Insurance Agency for violating the requirements set out in Article 32 of the GDPR with respect to its Employer Portal.[86] The Employee Insurance Agency has to be compliant by 31 October 2019.[87]
- The AP imposed, for the second time, an administrative enforcement order against the Dutch National Police for inadequate security of an IT system.[88] National Police has complied with the order.[89]

---

[80] See Question 9 on the additional enforcement powers provided for in the Implementation Act and the Awb.

[81] See also Question 10.

[82] Annual Report 2018, <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ap_bijlage_2018.pdf>, visited 2 August 2019.

[83] 'AP legt Uber boete op voor te laat melden datalek', https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-legt-uber-boete-op-voor-te-laat-melden-datalek>, visited 2 August 2019.

[84] 'Belastingdienst mag BSN niet meer gebruiken in btw-identificatienummer', <https://autoriteitpersoonsgegevens.nl/nl/nieuws/belastingdienst-mag-bsn-niet-meer-gebruiken-btw-identificatienummer>, visited 2 August 2019.

[85] Cf. Article 16(1) Dutch General Data Protection Regulation Implementation Act in conjunction with Article 5:32(1) Dutch General Administrative Law Act and Article 58(6) GDPR.

[86] 'AP dwingt UWV met sanctie gegevens beter te beveiligen', <https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-dwingt-uwv-met-sanctie-gegevens-beter-te-beveiligen>, visited 2 August 2019.

[87] 'AP dwingt UWV met sanctie gegevens beter te beveiligen', <https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-dwingt-uwv-met-sanctie-gegevens-beter-te-beveiligen>, visited 2 August 2019. See also <https://autoriteitpersoonsgegevens.nl/nl/nieuws/uwv-heeft-werkwijze-verzuimbeheer-aangepast-na-onderzoek-ap>, visited 2 August 2019.

[88] 'Nationale Politie beschermt politiegegevens nog steeds niet goed genoeg', <https://autoriteitpersoonsgegevens.nl/nl/nieuws/nationale-politie-beschermt-politiegegevens-nog-steeds-niet-goed-genoeg>, visited 2 August 2019.

[89] 'Nationale Politie voldoet aan last onder dwangsom', <https://autoriteitpersoonsgegevens.nl/nl/nieuws/nationale-politie-voldoet-aan-last-onder-dwangsom>, visited 2 August 2019.

In 2019, the AP issued a €460,000 fine to a hospital in The Hague for insufficient internal security of patient records, in a case where dozens of hospital employees had had access to the medical records of a Dutch TV celebrity. The AP found that the hospital did not use two-factor authentication and failed in control of logging (Article 32 GDPR). The hospital has announced that measures will be taken.[90]

Other violations found by the AP were stopped by other means such as informal enforcement action.[91] In 2018, the AP took informal action in 1,018 cases (298 data breaches and 720 complaints).[92]

Publication of sanctions

The AP has the power, based on the Dutch Freedom of Information Act[93] and in accordance with its publication policy guidelines, to publish, for instance, investigative findings and sanctions ordered against private companies or public authorities and other organisations, stating the name of the relevant organisation, even before a sanction has become final. The (primary) purpose is to inform and warn the public. Such publication by a supervisory authority is not to be considered as a sanction in itself[94], although this point of view is criticised in Dutch legal literature.[95]

Fining guidelines

On 14 March 2019, the AP published its new policy guidelines for calculating administrative fines.[96] In short, the AP divides infringements into several categories and assigns to each category a specific fine bandwidth and a 'basic fine' (the minimum of the bandwidth + 50% of the amount of the bandwidth). When calculating a fine, the AP will increase or decrease the amount of the basic fine depending on factors such as those referred to in Article 83(2) GDPR. The previously mentioned fine imposed on the hospital is the first example of the application of the new fining guidelines.[97]

Question 12:

Dutch law dictates that damages may consist of material loss or other disadvantages, though the latter only as far as the law implies that there is an entitlement to compensation. In that respect, by law the aggrieved party has a right of compensation for damages not consisting of material loss (such as injured honour or reputation) as well as a

---

[90] 'Haga beboet voor onvoldoende interne beveiliging patiëntendossiers', https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/haga-beboet-voor-onvoldoende-interne-beveiliging-pati%C3%ABntendossiers, visited 2 August 2019.

[91] Annual Report 2018, <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ap_bijlage_2018.pdf>, visited 2 August 2019.

[92] Annual Report 2018, <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ap_bijlage_2018.pdf>, visited 2 August 2019.

[93] See inter alia Administrative Jurisdiction Division of the Council of State 31 May 2006, ECLI:NL:RVS:2006:AX6362, point 2.7 and Administrative Jurisdiction Division of the Council of State 10 November 2010, ECLI:NL:RVS:2010:BO3468, point 2.5.

[94] See inter alia the Explanatory memorandum to the *Instellingswet ACM* (33 622), p. 57-58, Administrative Jurisdiction Division of the Council of State 2 August 2017, ECLI:NL:RVS:2017:2086, point 6.1 and District Court of Rotterdam 24 February 2017, ECLI:NL:RBROT:2017:5041, point 13.3. See also Court of First Instance 30 May 2006, Case T-198/03 (Lombard Club), ECLI:EU:T:2006:136 on the decision to publish the non-confidential version of a Commission decision.

[95] See e.g., Handhavingsrecht (HSB) 2016/5.4.2.

[96] 'AP past boetebeleidsregels aan', <https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-past-boetebeleidsregels-aan>, visited 2 August 2019.

[97] For that, see the EDPB Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237>, visited 2 August 2019.

harmed memory of a deceased (provided that the deceased himself, if he would still be alive, could have claimed damages for injuring his honour or reputation).

In contradiction with compensation for material loss – which is in principle subject to full compensation – the extent of the compensation for intangible harm is assessed in conformity with the standards of reasonableness and fairness. Judges in the Netherlands have a discretionary power in assessing the extent of the compensation, meaning also that they may choose not to award any compensation at all.[98] The judge may take into account all circumstances he deems relevant, taking into account the amounts that have been awarded by judges in similar cases. The judge may also take into account developments in surrounding countries, though these may never be decisive.[99][100]

Notwithstanding the above, compensation for intangible damages is not easily awarded in the Netherlands, in any case not in large sums. In a court ruling where freedom of speech was juxtaposed with the freedom to privacy, compensation was awarded to an employee of a phone company whose name was repeatedly mentioned in a blog post by an angry journalist who had had a bad experience with the customer service, more specifically with the aforementioned employee.[101] The court ruled that the employee suffered from injured reputation, as it was easy to find the (disproportionate) allegations against her via search engines, putting her in a negative light and possibly making it difficult for her to find a new job. Even though the court refers to the injury of reputation as being "substantially", only € 500 was awarded.

Question 13:
The Dutch Civil Code provides that a foundation or an association with full legal capacity can start legal proceedings aiming to protect similar interests of other persons, insofar as it is laid down in their statutes that they promote such interests.[102] In addition, the Awb provides for the possibility of the party / parties concerned to filed an objection in an administrative procedure, whereby a party concerned may also be a legal person that protects general or collective interests following their stated purposes or factual activities.[103]

The UAVG provides though that a processing activity cannot be subject to legal proceedings under the Civil Code nor a formal objection in an administrative procedure under the Awb, if the person that is affected by the processing activity has objections against this.[104] This means that representative actions may only be initiated if the affected person(s) do not object. At the time of writing, no examples of such cases are until now available.

There are however several NGOs and initiatives in the Netherlands that play an important role with regard to pursuing the public interest in relation to privacy and the protection of personal data.

[98] HR 27 April 2001, NJ 2002/91.

[99] HR 17 November 2000, NJ 2001/215.

[100] Besluit vergoeding affectieschade.

[101] Rb. 's-Gravenhage 21 November 2007, KG 07/1158.

[102] Article 305a Civil Code - https://wetten.overheid.nl/BWBR0005291/2019-01-01/#Boek3_Titeldeel11_Artikel305a

[103] Article 1:2 3rd indent Awb - https://wetten.overheid.nl/BWBR0005537/2019-04-02/#Hoofdstuk1_Titeldeel1.1_Artikel1:2

[104] Article 37 UAVG

Bits of Freedom has, for example, developed a tool called “My Data Done Right”. With this tool, over 17.000 people filed a request to get access to their data. Also, it organizes an annual and widely media-covered event giving a Big Brother award to the person or organization that has been deemed the biggest violator of privacy of that year.

Civil society has also campaigned for organizing a consultative referendum on the Dutch Intelligence and Security Services Act (In Dutch: *Wet informatie en veiligheidsdiensten*, or *Wiv*). Of the 6,7 million Dutch inhabitants that voted in this referendum, a majority voted against. Although the referendum was not binding, the government did adjust the Wiv to meet some of the worries of the public.

A last example where civil society organized is when a broad coalition of civil society organizations went to court to have the Dutch Implementation Act of the Data Retention Directive, the Dutch Data Retention Act, invalidated. On 11 March 2015, the district court of the Hague indeed rendered the Dutch Data Retention Act invalid.[105]

Question 14:
The AP does cooperate in the national context with different other supervisory authorities and has signed cooperation agreements laying down the cooperation arrangements.[106] Usually a covenant is used to lay down how the supervisory authorities will cooperate and how they share the tasks and reach the goals that they have in common and for which they may cooperate. The AP has signed a covenant with the following organisations:

- The Dutch Media Authority (in Dutch: *Commissariaat voor de Media*)
- The Dutch central bank (in Dutch: *De Nederlandsche Bank*)
- The health and Youth Care Inspectorate in formation (in Dutch: I*nspectie Gezondheidszorg en Jeugd in oprichting (IHJ i.o.)) –*
- The Consumer and Market Authority (in Dutch: *Autoriteit Consument en Markt (ACM)*)
- The Dutch Healthcare Authority (in Dutch: *Nederlandse Zorgautoriteit*)
- The Inspectorate of Education (in Dutch: *Inspectie van het onderwijs*)
- The government service for identity data, which is *Rijksdienst voor Identiteitsgegevens*
- Radiocommunications Agency (in Dutch: *Agentschap Telecom*)

Arguably, the cooperation between the ACM and the AP is the most relevant one with regard to the protection of personal data, as these two authorities have a shared responsibility concerning the use of personal data in relation to Dutch implementation of the ePrivacy Directive. The cooperation agreement mainly regulates the general exchange of information between the authorities and situations in which their competences overlap

[105] https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2015:2498

[106] https://www.autoriteitpersoonsgegevens.nl/nl/over-de-autoriteit-persoonsgegevens/nationale-samenwerking

Another covenant that warrants specific mention is the recently signed covenant between de AP and the DNB. Following the introduction of the Payment Services Directive 2[107], where third parties may get access to the banking details of a consumer after (s)he has given his / her consent, the AP and the DNB have entered into an agreement in which they demarcate their responsibilities towards the use of banking information.

In addition to bilateral agreements with the mentioned organizations, the AP also participates in the Markttoezichthoudersberaad , which is the meeting of regulators who (partly) focus on the functioning and behavior of market players. In addition to the AP, also the ACM, Financial Market Authority, The Dutch Media Authority, the DNB, the Netherlands Gambling Authority and the Dutch Healthcare Authority participate in the MTB.

The Dutch Ombudsman helps citizens whenever an issue arises between a citizen and public authorities. He defends the interests of citizens and help public authorities to improve their service. The Ombudsman does this by referring, mediating or investigating a specific issue. This may mean that a case is being referred to the AP in case the AP is in a better position to help the citizen. At the same time, the Ombudsman is also able to hear and investigate complaints about the AP by citizens.

Question 15:
The Dutch Government has concluded that the processing of personal data for national security purposes as derogation from the regimes provided by the GDPR and the Law Enforcement Directive coincides with the processing of data as part of the work of the intelligence and security services.[108]

The UAVG "does not apply to the processing of personal data referred to in Article 2(2) of the GDPR."[109] However, by means of exception, it does apply , "to the processing of personal data […] in the course of an activity which falls outside the scope of Union law"[110]. However, the processing of personal data by or for the benefit of the Military Intelligence and Security Service and the General Intelligence and Security Service (in Dutch: *AIVD*) in relation to their tasks is again excluded.[111]

As a result, personal data processed by a private party but destined for use by one of the intelligence services does not fall within the scope of the UAVG nor the GDPR. However, the GDPR is applicable to the processing of personal data by other public bodies in the interest of national security, for example the processing as part of the performance of the tasks and

[107] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, OJ L 337/35.

[108] EM UAVG, paragraph 2.2, https://www.rijksoverheid.nl/documenten/kamerstukken/2017/12/13/memorie-van-toelichting-uitvoeringswet-algemene-verordening-gegevensbescherming, last accessed 20 June 2019

[109] Section 2, paragraph 3, of the GDPR Implementation Act.

[110] Section 3, paragraph 1, sub a), and paragraph 2 of the GDPR Implementation Act. Article 2(2) under a) of the Regulation is thus brought within the ambit of the Implementation Act and the GDPR.

[111] EM UAVG, paragraph 2.2, https://www.rijksoverheid.nl/documenten/kamerstukken/2017/12/13/memorie-van-toelichting-uitvoeringswet-algemene-verordening-gegevensbescherming, last accessed 20 June 2019.

competencies incumbent to the Minister of Justice in the interest of national security (for instance counterterrorism).[112]

The Wiv does not provide a detailed definition of the term 'national security'. It follows from the definition of the tasks of the AIVD that national security coincides with the maintenance of the democratic legal order, with security or with other important interests of the Dutch state.[113] Concerning the Military Intelligence and Security Service, the protection of national security requires mainly the maintenance of the international legal order and the readiness of the armed forces.[114]

The processing of personal data covered by the Wiv is broadly defined.[115] It encompasses data related to persons concerning whom there is a serious suspicion that they form a threat to the democratic legal order, to security or to other important interests of the Dutch state.[116] Data concerning enquiries or analyses related to other states and data related to persons who have been examined by foreign intelligence services fall under the Wiv as well.[117] Personal data necessary for the correct functioning of the services can also be processed under the Wiv, even as personal data needed to perform more general analyses of threats and risks.[118] Not only data concerning the persons directly related to these goals, but also to persons involved more indirectly can be collected when they form an inextricable part of a larger set of data.[119]

According to the AIVD the Wiv not only applies to names and addresses of its targets, but also data related to its suppliers and to applicants or persons or companies related to the service in any other way. [120] The AIVD indicates as well that certain categories of private companies, for instance providers of telecom services, have the legal obligation to provide data to the security services when required. They are not allowed to inform, amongst others, the person concerned of the transmission of these data.[121] This corresponds to the aforementioned explanation by the Dutch government that the GDPR does not apply to data intended for the security services, even if they are collected and transmitted by an external actor.

The laws implementing Directive (EU) 2016/680 do not define the terms 'national security' either. They apply, in brief, to the processing of personal data for police tasks, personal data in relation to criminal law and criminal procedure and personal data processed by the public prosecutor for the purpose of a criminal investigation. The Police Data Act provides for the transmission of personal data to the two aforementioned intelligence services for the

---

[112] Idem, see also H.R. Kranenborg and L.F.M. Verhey, *De Algemene Verordening Gegevensbescherming in Europees en Nederlands perspectief*, Deventer, Kluwer 2018, p. 126.

[113] Section 8, paragraph 2, sub a) of the Intelligence and Security Services Act 2017.

[114] Section 10, paragraph 2, sub a) of the Intelligence and Security Services Act 2017.

[115] Section 19, paragraphs 1, 2 and 5 of the Intelligence and Security Services Act 2017.

[116] Section 19, paragraph 1, sub a), of the Intelligence and Security Services Act 2017.

[117] Section 19, paragraph 1, sub c) and d), of the Intelligence and Security Services Act 2017.

[118] Section 19, paragraph 1, sub e) and g), of the Intelligence and Security Services Act 2017.

[119] Section 19, paragraph 5, of the Intelligence and Security Services Act 2017.

[120] https://www.aivd.nl/onderwerpen/aivd-en-privacy/documenten/publicaties/2018/05/25/naar-aanleiding-van-bescherming-van-persoonsgegevens-met-de-avg

[121] Idem.

purpose of the fulfillment of their tasks.[122] This possibility or obligation is contained as well in the Wiv.[123]

Application of the EU Charter of Fundamental Rights
According to the Explanatory Note to the Wiv, the acts of the intelligence and security services fall, pursuant to article 4, paragraph 2, TEU, outside the scope of the powers of the Union. Hence, the processing and retention of personal data by these services do not fall under the EU privacy legislation. The Charter is only applicable to the implementation of EU law by the Member States.[124] The privacy rights of the constitution and the ECHR are however applicable.

The Council of State considered in this respect that EU law and the case law from the Court of Justice do not apply to the intelligence and security services. However, it is likely that the principles developed by the ECJ are relevant for the scope and limitation of their powers.[125] This significance will develop through the incorporation of the relevant ECJ case law in the European Court of Human Rights case law.

The judiciary seems to share this point of view in a ruling that concerns transmission of bulk data from foreign intelligence services to the Dutch Government. According to the Hague District Court, EU law does not apply to these intelligence operations.[126] This same court ruled as well, in summary proceedings regarding the validity of certain sections contained in the Wiv, that this Act contains rules related to the security and intelligence services. This is a domain, according to the Court, preeminently excluded from the scope of application of EU law by article 4, paragraph 2, TEU. Therefore, the Court did not deem necessary to refer preliminary questions to the ECJ.[127]

[122] Section 24 of the Police Data Act.

[123] Sections 91-94 of the Intelligence and Security Services Act 2017. This obligation to cooperate with the security and intelligence services, also exists for the military police, the tax authorities, the social security services and the immigration office. Section 93 provides for the transmission of data by the Prosecutors office.

[124] E.M. Intelligence and Security Services Act 2017, p.250, https://www.rijksoverheid.nl/documenten/kamerstukken/2016/10/28/memorie-van-toelichting-inzake-wijziging-wet-op-de-inlichtingen-en-veiligheidsdiensten, last accessed 22 June 2019.

[125] Opinion from the Council of State regarding the draft Intelligence and Security Services Act 2017 and explanatory memorandum https://www.raadvanstate.nl/@64162/w04-16-0097/.

[126] The Hague District Court, 23 July 2014, ECLI:NL:RBDHA:2014:8966, point 5.24. See also, for more information on this case: https://fra.europa.eu/sites/default/files/fra_uploads/netherlands-study-data-surveillance-nl.pdf, page 3, paragraph 6.

[127] The Hague District Court, 26 June 2018, ECLI:NL:RDBHA:2018:7459, point 4.1.