pro facto

Verkennend onderzoek

De verwerking van politiegegevens in vijf Europese landen

Groningen, 20 november 2020

www.pro-facto.nl

Ossenmarkt 5
9712 NZ Groningen

profacto@pro-facto.nl
050 313 98 53

rijksuniversiteit groningen

Colofon

Het onderzoek is – in opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) – uitgevoerd door Pro Facto, bureau voor bestuurskundig en juridisch onderzoek, advies en onderwijs, en de vakgroep Staatsrecht, Bestuursrecht en Bestuurskunde van de Rijksuniversiteit Groningen.

Projectleider:	prof. dr. Heinrich Winter
Onderzoekers:	Joachim Bekkering (LLB; onderzoeksassistent), mr. Tinka Floor, dr.ir. Bieuwe Geertsema, mr. Stef Roest en dr. John Smits
Met medewerking van:	prof. dr. Jeanne Mifsud Bonnici
Begeleidingscommissie:	prof. mr. G.K. Sluiter (voorzitter), dr. C.H.M. Geuijen, dr. B. Van der Sloot, mr. C.A.N. Huisman, dr. L.M. van der Knaap

Summary

Purpose and accountability
This exploratory study was carried out on behalf of the WODC (Research and Documentation Centre of the Dutch Ministry of Justice and Security), and comprises an inventory of the various options for regulating the processing of police data in legislation. The aim of the study is to provide insight into how the legal framework for the processing of police data is designed in five other European countries and how that framework relates to the European basic principles. The findings from this study can serve as input for the revision of the Police Data Act (Wet politiegegevens, Wpg). The following two main questions are central to this research:

- *What is the current state of affairs in the Netherlands with regard to the legislation for processing police data, to what extent have the previously identified problems been resolved and what problems remain? How has the Netherlands implemented the European framework for the processing of data by the police?*
- *What is regulated in the legislation for the processing of police data in other European countries, how have these countries overcome the problems that exist in the Netherlands and any other problems through legislation, and how has the European framework for the processing of data by the police been implemented?*

This leads us to the following subquestions:

1. What is the current state of affairs in the Netherlands with regard to the legislation on the processing of police data, to what extent have the previously identified problems been resolved and what problems remain?
2. On what grounds are police data obtained in other European countries?
3. What frameworks are there in other European countries for the processing of police data? To what extent does legislation focus on new technological developments, for example in the field of linking files and the use of methods and techniques for analysing big data?
4. What frameworks are in place in other European countries for providing police data to third parties, and is a distinction made between different parties?
5. What retention periods and destruction conditions apply in other European countries? Is a distinction made between types of data or different purposes?
6. How, in other European countries, is the supervision of the processing of police data arranged by law.
7. Are police data in other European countries 'labeled' or 'categorized' and if so, which labels are used (e.g. factual data, soft data, sensitive data, etc.)?
8. How do the answers to the above questions relate to the European legal framework for processing police data, in particular the Directive on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution (Directive 2016/680)?

In order to answer main question 1 and ask relevant questions in the countries to be studied, it was important to have a clear picture of the current legal framework in the Netherlands for processing police data. The data required for this were collected by means of desk research and four interviews with key informants from the police, the Royal Netherlands

Marechaussee (Kmar) and the Ministry of Justice and Security and an expert from the academic world.
Five European countries were selected by means of a quick scan and predefined criteria. The selected countries are Belgium, Denmark, Germany, Finland and Ireland. Desk research was carried out in each country to look at the legislation in each reference country. The information obtained was then examined in more detail, tested and supplemented with (practical) information from interviews with people from the police, supervisors, policy officers from the responsible department and independent academic experts. Only in Denmark has it not been possible to speak to all the intended parties. It is important to note that due to the short duration and limited aim (mainly studying the legislation) of this study, it was not possible to form a complete picture of the implementation practice in each reference country.

Problems in the Netherlands
The sub-study in the Netherlands shows that the Wpg has hardly changed, in a rapidly developing digitized world, since its entry into force in 2008. Developments such as the transition to a single National Police Force, digitization, technology and the implementation of the Directive on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution have not resulted in a (radical) revision of the Wpg. It is therefore not surprising that some problems identified during the evaluation of the Wpg in 2013 remain. In addition, new problems have also arisen. The main problems are:

Legislative system: compliance with the Wpg and the extent to which the Wpg lends itself to compliance

The Wpg is difficult to comply with because it contains many open standards, is perhaps too detailed on other points and is not very aligned with implementation practice and organization/ICT. Additionally, the Wpg was originally written for the processing of data by and the exchange of data between regional police forces within the Netherlands. Neither has the implementation of EU Directive 2016/680 improved compliance with the Wpg. The Directive applies to the *prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties (including the safeguarding against and the prevention of threats to public security*) by competent authorities. The Wpg defines police data, just as in the time prior to the Directive, as *any personal data that are processed in the context of the performance of the police task.* However, there are exceptions to this. For example, with the entry into force of the European framework, a number of tasks now fall under the GDPR. Art 2 Wpg declares the Wpg applicable to the processing of police data by a competent authority, whereby a 'competent authority' is defined based on the police tasks referred to in the Police Act 2012 and art. 1 sub a Wpg, rather than using the definition set out in the Directive. This creates confusion and demarcation problems.

Legislative system and data processing: the categorization of police data

Police data are categorized by police task on the basis of the Wpg (art. 8-13 Wpg). Each category has a processing regime with a retention period that, in practice, creates 'surplus'. This is not practical for police work because data can fall into several categories and the role of the data subject can differ per case, making it unclear which regime should be applied.

Legislative system: concurrence with other legal regimes for data processing

The Wpg overlaps and has interfaces with various other laws and regimes for data processing. This creates a lack of clarity, for example when providing data to parties that fall under the GDPR.

Acquiring data: basis for acquiring data is too restrictive for police work

Art. 3 of the Police Act 2012 (description of the police task) is often the basis for acquiring data collected with new techniques to maintain public order. An example of this is the use of the bodycam. However, this general article only acts as a legal basis if there is a minor breach of privacy; more serious breaches require a specific legal basis.

Digitization and technology

There are more and more data available from more and more different sources. For example, the internet, drones and bodycams. There are also more and more possibilities to analyse data (on a large scale). On the other hand, according to (European) privacy legislation, a specific legal regulation is required for every breach of privacy. The question is, how can Dutch legislation comply with this and at the same time last for a longer period of time without becoming outdated with every new technological development?

Retention of data: multiple dilemmas with retention periods

Data can fall under different processing regimes, which means that multiple retention periods apply to the same data. In addition, retention periods have been included in various laws, so it is not always clear how long data may be retained. The police also experience tension between the importance of privacy and concern about losing information valuable for police work. As a result, data are retained for too long.

Provision and sharing of data: semi-closed provision regime of the Wpg incompatible with the need for cooperation

Sharing police data outside the Wpg domain is only possible in exceptional cases due to the semi-closed regime of the Wpg. This regime is not (any longer) in line with the level of cooperation between the police and other parties in the Netherlands. On the other hand, police data often consists of sensitive and sometimes soft information, and it is sometimes difficult to distinguish between fact and opinion.

Provision and sharing of data: checking safeguards when disclosing to third countries is cumbersome

Provision to third countries on the basis of art. 17a Wpg can be a problem. The BES islands (Bonaire, Saint Eustatius and Saba) also fall under these third countries. If it has not previously been established that the third country/international organization falls under art. 17a paragraph 2, the controller must each time weigh up the need for disclosure and the infringement of the rights of the data subject. This system can cause problems in practice, especially when cooperation with a country is required on the basis of a certain security problem, but the country in question does not offer the appropriate privacy safeguards.

Supervision: external supervision still has open ends

The Personal Data Authority (AP) does not have the authority to stop processing or to delete unlawfully processed data. The question is whether the powers of the AP are sufficient. In addition, discussion partners say that the AP has insufficient manpower and means to supervise.

The Dutch problems in the reference countries

Legal system

The legal system in the reference countries differs. Some countries have opted to convert/implement both the GDPR and the Directive into a national privacy law. Other countries have implemented the Directive through a separate transposition law, with some countries opting

for additional legislation per competent authority. Germany had already included a section on data processing in each police act (at least at Federal level and in North Rhine-Westphalia).

The legislation in all reference countries is based on the protection of personal data, as defined in European law, by the police and other competent authorities. The term 'police data' and the legal system opted for in the Netherlands does not seem to be used elsewhere. The term 'competent authorities' in the Directive is interpreted differently in the reference countries: Belgium, Denmark and North Rhine-Westphalia explicitly name the competent authorities, while other countries follow the definition of the Directive literally and do not specify it further. In Ireland, for example, whether the action falls under the Directive has to be determined on a case-by-case basis.

The collection, use or sharing of data is only lawful under European and national regulations if there is a legal basis for this and it is necessary for the purpose. Such a purpose and legal basis may be the performance of a police task described by law. In the reference countries, data are not categorized 'statically' according to the police task and the corresponding purpose ('daily police task', investigation in a specific case, etc.), as in the Netherlands on the basis of art. 8-13 Wpg, but the police task is used as a basis when assessing the purpose limitation, necessity and proportionality of the processing of personal data. Personal data can therefore be used for purposes other than those for which they were collected, provided this fits within the task field of the police; the reference countries are less affected by surpluses due to the categorization of data.

Acquisition

The bases for obtaining police data in the reference countries largely correspond with the Dutch bases. The general conditions and safeguards are based on the European principles of data protection. The reference countries have many different specific legal bases for police action in special laws (in addition to the general basis in privacy law, police law and the criminal procedure code) to justify a breach of privacy. The emphasis that the countries place in this respect differs: one country puts more emphasis on the information position of the police, the other country more on the protection of personal data.

Digitization

When it comes to digitization and technology and the acquisition of personal data, all countries experience the same problem as the Netherlands. Each country tries to take into account the rapid technological developments by formulating the legislation as 'technology-neutral' as possible, while at the same time the legislation must be as specific as possible from a fundamental rights perspective.

In the reference countries, we also investigated what powers authorities have once data are in their possession (options for processing police data). Given the Dutch problems, the focus was on (technical) use and analysis options, including use for purposes other than those for which the data were obtained. Most of the countries have adopted the Directive almost literally on this point. The countries choose not to give further substance to the technological possibilities. The reference countries do, however, have general guidelines for the use of new techniques. These guidelines often concern necessity, proportionality, purpose limitation and appropriate technical and organizational security measures. In practice, this leads to restraint and caution in the use of new technological possibilities in the processing of personal data.

Editing

In the Netherlands, police data are categorized by police task. This makes editing data (in this study defined as: using data for a purpose other than that for which it was collected) difficult. With the exception of Germany, the reference countries set less stringent requirements for this. For instance, the editing of data is possible when the new purpose fits within the task field of the police and the judiciary. In Germany, strict conditions apply to processing data for a purpose other than that for which they were obtained. At the very least, there must be an equally serious criminal offence or an equally important interest or legal claim ('principle of hypothetical re-collection of data').

When editing police data, it is important that data are clearly categorized and labeled. The reference countries have adopted the mandatory categorization of personal data from the Directive into their legislation and have often added categories to it. In practice, however, the same problems still arise as in the Netherlands: the distinction between fact and opinion is sometimes difficult to make, and the role of the data subject may differ per case. In addition, large datasets do not lend themselves to categorization because the requirements for categorization are more tailored to individual cases.

Retention and destruction

The rules on the deadlines for retaining and deleting/archiving/destroying data differ in the reference countries. In Belgium and Finland, rules have been laid down by law with regard to retention periods and grounds for destruction. In Germany, Denmark and Ireland this is mainly laid down in protocols of competent authorities and left to the discretion of the professional in the individual case. Germany lays down certain maximum periods (for checking whether data should/may be kept longer) in legislation.

Provision and sharing

In all reference countries, three types of disclosures of police data within the country can be distinguished: disclosures to other authorities within the regime of the Directive, disclosures to authorities with a public and legal task for which data sharing is appropriate, and disclosures to other organizations and persons. The Directive applies to the first group and the conditions are set at a low level. The conditions and requirements for the other two groups differ in the reference countries. However, a certain form of regulation has always been drawn up in the form of agreements for the provision to and/or sharing with these two groups.

In the case of disclosure in the international sphere, the Directive is leading, with the result that the same debate as in the Netherlands is going on in each country with regard to disclosure to third countries. The Danish situation is particularly interesting for the Netherlands in this case, because Denmark, like the Netherlands, has overseas territories outside European territory. These areas are regarded as third countries, which means that data cannot be automatically shared. Denmark is therefore working on the implementation of sufficient data protection rules in those areas to get an adequacy decision from the European Commission. It is also important to point out that, following up case law of the Federal Constitutional Court (Bundesverfassungsgericht), Germany has included in the legislation an additional test of the rule of law and human rights that must be carried out before sharing data with (parties in) third countries.

Supervision

In the reference countries, external supervision is often entrusted to a general authority that supervises both the GDPR and the Directive. Only Belgium deviates here: it has an external supervisor specifically for the implementation of the Directive. This supervisor already existed

in a slightly different form before the implementation of the Directive and was established because a special supervisor could deploy more expertise with regard to the work of competent authorities. In all reference countries, it appears that the supervisor often uses soft means when it has to act against the processing of personal data. In contrast to the AP, the external regulator does have the option in many countries to intervene sharply, for example by having the processing operations stopped. In practice, however, this remedy is hardly used because it is considered to be too drastic.

With regard to the access of data subjects to the data collected and processed about them, all countries except Belgium follow the Directive. Belgium uses the system of 'indirect access'. This means that the supervisory authority processes the request for access, passes it on if necessary and only provides limited information about the processing of data to the data subject. Whether this interpretation of the Directive is tenable is very questionable.

Follow up
This exploratory study provides the Dutch legislator with starting points for adapting Dutch legislation and a possible starting point for further research into the described developments that are taking place in other countries and choices that are made elsewhere. This study could be expanded by including the implementation practice in the reference countries to a larger extent.

pro facto