TRANSLATION OF THE OFFICIAL PUBLICATION OF SINT MAARTEN

EXPLANATORY MEMORANDUM

GENERAL SECTION

The structure, organisation and management of the police of Curaçao, Sint Maarten, and of Bonaire, Sint Eustatius and Saba is regulated in the Police Kingdom Act of Curaçao, of Sint Maarten, and of Bonaire, Sint Eustatius and Saba[1]. Article 39(1), of the Police Kingdom Act of Curaçao, of Sint Maarten, and of Bonaire, Sint Eustatius and Saba requires the police forces of Curaçao, Sint Maarten and of Bonaire, Sint Eustatius and Saba to exchange police data if this is necessary for good performance of police tasks. Paragraphs 4 and 5 of Article 39 make the same provision for the exchange of police data between the police forces of the European section of the Kingdom and Curaçao or Sint Maarten. The aforementioned exchange takes place in observance of the national regulations applying for this.

Article 39(2) provides that the countries, in the interests of the exchangeability of police data, must reach a mutual arrangement by which police data are processed, including the orthography and classification of data and the method for reporting the source of data. It follows from Article 57 of the draft Police Kingdom Act of Curaçao, of Sint Maarten, and of Bonaire, Sint Eustatius and Saba that, pending regulations to protect personal data – i.e. pending the entry into force of paragraphs 4 and 5 of Article 39 – a mutual arrangement will be agreed for the exchangeability of police data between Curaçao, Sint Maarten and the European section of the Kingdom, imposing further rules regarding the protection level. These regulatory orders have been combined in a single mutual arrangement.

The relevant mutual arrangement has already been established and, until this draft National ordinance police data enters into force, shall ensure that the countries can rely on each other to ensure that the processing of 'their' police data complies with certain (minimum) conditions after being passed on to another country.

In the preparation of this draft, a decision was made to base the preparation of this draft national ordinance on the Dutch Police Data Act. The question of whether that legislation is adequate for Sint Maarten was continually asked and answered. Other relevant (Dutch) legislation has also been considered. This concerns regulations that provide for the processing of personal data in a more general sense, such as regulations directed at the exchange of personal data and the assurances necessary for such an exchange. At present, for example there are a Data Exchange Protocol between the Netherlands Antilles and the Netherlands and a Regulation concerning police registration of data exchanges concerning crimes in the Kingdom. At the international level, too, there are legal instruments relevant to Sint Maarten, the subject of which is the processing of personal data. Convention No. 108 of 28 January 1981, for the Protection of Individuals with regard to Automatic Processing of Personal Data, has been agreed within the Council of Europe.

THE DRAFT IN OUTLINE

Introduction

The aim of this draft national ordinance is to provide scope for the processing of data for the optimal performance of the police tasks, with respect for the principles aimed at the protection of personal privacy. The draft entails a balance between protection of the privacy of citizens on the one hand and the interests of law enforcement on the other. A choice has been made for statutory possibilities for the storage, use and provision of personal data by the police and assurances for citizens against unlawful breaches of their privacy.

[1] Parliamentary Documents II 2008-2009, 32019 (R 1886), No. 2.

Data protection principles

As mentioned above, inspiration for the structure and content of this regulation was sought in existing relevant regulations. All these regulations are based on the same principles concerning data protection.

Purpose-specification
'Purpose-specification' means that personal data are gathered for a predetermined purpose and are then processed further for that purpose. Articles 11 up to and including 16 concern purpose-specification. In principle, police data are processed only if necessary for the proper performance of police tasks.

Quality, proportionality and lawful acquisition
Personal data that are processed must be accurate and current. No more data may be processed than are necessary for the purpose for which they are gathered. Data that are no longer necessary for that purpose should be destroyed. Furthermore, the data must be gathered in a lawful manner. Articles 3 and 4 reflect these principles.

Transparency
The person concerned has a right to know whether his data are processed, and the purpose of this. To that end, he may submit a request for viewing pursuant to Article 27. Such requests need not be met in all cases. Article 29 formulates the exceptions that the person responsible may invoke.

Rights of the persons concerned
In addition to the right of access (viewing), a person concerned must have the right of correction, supplementation and deletion of his data. These rights are laid down in Article 30.

No processing of sensitive data
Barring some exceptions, personal data that reveal something concerning a person's religion or faith, race, political views, health, sexual life or trade union membership may not be processed. This mutual arrangement permits the processing of sensitive police data only as a supplement to the processing of other police data, to the extent that this is unavoidable for the proper performance of police tasks. Article 8 standardises the processing of sensitive police data.

Security and authorisation
Good physical and organisational security is essential to be able to process personal data lawfully (Article 4). A good system of authorisation forms part of this (Article 9). The same applies for the confidentiality obligation (Article 10).

Adequate level of compliance
Obviously, compliance with the rules concerning the processing of personal data is also required. There are different instruments that can contribute towards this. Firstly, citizens must have the possibility of taking action against unlawful processing, by filing objections or appeals, by taking legal action, by submitting a complaint to a supervisory authority and by claiming compensation for damages. Secondly, it is important that there is external supervision of the persons responsible. Article 33 provides for this. Thirdly, the persons responsible must be well aware of their obligations and the rights of the persons concerned. Privacy awareness by police officers is of crucial importance for good compliance with the agreed rules. This is partly a matter of education and public data in the countries.

Strasbourg criteria

When police data are processed by the police, the right to protection of personal privacy may be at issue. In order to avoid a disproportionate breach of the privacy of citizens in the performance of police tasks, the draft provides for rules for treating the data with due care. International regulations have been observed here. The principles for data protection are laid down in the Convention of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981). This concerns principles that mean that data must have been obtained lawfully, may be saved for specific and legitimate purposes only, must be proportionate in

relation to the objective for which they have been saved and may not be saved for longer than is required for the purpose for which they have been saved. The requirement of purpose-specification means that personal data are used only for the purpose for which they are gathered. Logically, purpose-specification must be accompanied by a description of the purpose. The purpose must be specified, explicitly described and justified. The use of the data for a different purpose is acceptable to the extent that such use is not inconsistent with the purpose for which the data was gathered. Sensitive personal data (regarding race, political views, faith etc.) are not processed unless the national legislation provides for the necessary assurances. Derogation from the principle of purpose-specification is possible if this is necessary in a democratic society in the interest of (among other things) the control of criminal offences. Article 3 of this national ordinance provides that personal data are obtained for specified, explicitly described and justified purposes. This means that no data may be gathered without a precise purpose. In this draft national ordinance, the purpose-specification is developed for the tasks of the police, which form part of the police tasks referred to in Article 5 of the Kingdom Act. The convention discussed above develops Article 8 of the European Convention on Human Rights (ECHR) in the field of data processing. The explanation provided for Article 8 of the ECHR is important for an explanation of the convention and for the definition of certain terms in the convention. The criterion arising from the convention that the processing of data by the police must be necessary for the proper performance of police tasks is consistent with the criterion in Article 8(2) of the ECHR, which means that restriction of the right to respect for personal privacy is permitted only to the extent that this 'is necessary in a democratic society' in the interests of a number of specified objectives, including the prevention and detection of criminal offences. The term 'necessity' plays an important role in this convention with regard to the limitation of the core powers to process, authorise and provide data. The necessity criterion is developed further in the Strasbourg jurisprudence with the requirements of proportionality (are the interests of the processing in proportion to the restriction of personal privacy?), of a 'pressing social need' (there must be a pressing social need to realise the legitimate objective) and subsidiarity (are other measures that intervene less in the personal privacy of the citizen reasonably possible and sufficiently effective?). The relevant responsible authority must always consider, with regard to proposed processing, authorisation and/or provision of data, the extent to which the action is 'necessary'; the aforementioned Strasbourg criteria must be applied here. The legitimacy of the defined objective is not sufficient in itself; the necessity requirement is cumulative. The assessment of the necessity of the processing of police data entails an assessment margin that lies somewhere between 'essential' as the upper limit and 'normal', 'useful', 'reasonable' and 'desirable' as the lower limit.

The draft complies with the requirement of foreseeability by linking the processing of police data to specific objectives described in advance and, to the extent that processing pursuant to Article 12 is involved, by determining the categories of persons concerning which personal data may be processed. Article 8 of the ECHR and the jurisprudence based on it also impose requirements for the quality of the legal regulation. These mean that the legal regulation must be sufficiently accessible and identifiable for the citizen. These requirements mean that the regulation must be formulated in a sufficiently precise manner, so that citizens can know in advance the circumstances and conditions under which personal data may be processed. The regulation must also provide for assurances against random government intervention in the personal life of the citizens and against the abuse of powers. This means that the law must describe the cases in which, and the purposes for which personal data may be processed. The designation of the competent authority and provisions for transparency and controllability, such as reporting regulations, are also important.

ARTICLE-BY-ARTICLE SECTION

Article l
This Article defines a number of terms that are regularly used in the national ordinance and the provisions based on it. The most important ones are explained below.

Police data
The key term in this national ordinance regulation is the item of police data. An item of police data is an item of data that relates to a natural person who is known or whose identity can be traced. In other words, it is an item of personal data, an item of data that says something about a natural

person. Only personal data that are processed with a view to performance of police tasks are defined as police data.

Processing
The term 'processing' covers all possible actions that can be performed with regard to police data. Processing generally starts with the gathering and storage of items of data and ends with their destruction.

Provision
The definition of 'provision' matches the scope of this national ordinance and is therefore confined to the exchange of police data between the persons responsible.

Person concerned
The person concerned in the natural person to whom an item of police data relates, such as a suspect or a witness.

Processor
A processor is someone who processes police data for the person responsible, without being their subordinate or standing in a hierarchical relationship to the person responsible in other ways. A (police) officer in the employ of the person responsible is not, therefore, a processor. A company that is engaged to manage data is a processor. However, for security reasons, a processor is far less likely to be engaged to process police data than is the case for processing other personal data, for example personal data of clients of a mail order company. If a person responsible makes use of the services of a processor, the latter must comply with certain conditions.

Article 2
Article 2 describes the scope of the draft. The draft applies to all data obtained in relation to the performance of police tasks pursuant to Article 5 of the Police Kingdom Act of Curaçao, of Sint Maarten, and of Bonaire, Sint Eustatius and Saba.

Paragraph 2
In this paragraph, the application of this national ordinance is ruled out for data that is processed solely for personal purposes. This concerns, for example, working notes that serve as a memory aid and that are recorded in diaries, on notepads and the like. However, the provision or supply of such working notes with a view to performing police tasks deprives those notes of their personal character. It also follows from the linking of the processing to the police tasks that the National police data does not apply to personal data that are processed for the internal operations of the police force. The purpose of Article 2(2)(b) is to eliminate any doubts in that regard. The internal operations refer to data processing relating to the internal organisation of the police force, such as the personnel and salaries administration.

Article 3
Pursuant to paragraph 1, the police are not permitted to process personal data unless this is necessary for the purposes formulated by or pursuant to this national ordinance. Pursuant to paragraph 2, the police are not permitted to process data that have been obtained unlawfully. Unlawful acquisition may refer to e.g. data obtained in a situation where certain provisions of criminal law were violated, or data obtained in contravention of the provisions applying pursuant to this draft. An important principle for the protection of personal privacy is the principle of purpose-specification, which is developed in paragraph 1. The draft aims to provide an exhaustive list of the purposes for which police data may be processed. Paragraph 3 reflects the fact that the use of police data in derogation from its purpose within the police force is possible only if the draft makes explicit provision for this.

Article 4

Paragraph 1
This paragraph provides that the person responsible must take measures to ensure that police data are correct and accurate. This involves an effort obligation. After all, establishing the accuracy of data that are often unconfirmed is part of the tasks of the police. As soon as certain data that the

police processes proves to be incorrect, it must be destroyed or corrected. Paragraphs 2 and 3 also concern an effort obligation.

Paragraph 2
This paragraph requires the person responsible to take the necessary measures to ensure that data are removed or destroyed as soon as it is no longer necessary for the purpose for which it has been processed. The draft also regulates terms, on the expiration of which the data may no longer be processed. As soon as these terms have expired, the relevant data must be removed or destroyed.

Paragraph 3
This paragraph includes an obligation for the person responsible to ensure that the automation contains sufficient assurances to prevent data from remaining in the system longer than is warranted pursuant to the national ordinance.

Paragraph 4
In order to enable the manager to realise his responsibility for correct and secure processing of police data, this paragraph provides that the person responsible has access to police data for that purpose.

Articles 5 up to and including 7
The inclusion of these Articles relates partly to the introduction of the role of the processor in this draft (Article 4(5)). The processor takes no decisions regarding the processing of personal data, must comply with its instructions from the person responsible with regard to technical and organisational measures to secure personal data and is in principle liable for any damages arising through its work.

Article 8
Sensitive data may be processed, to the extent that it has a clear function in the performance of police tasks. If, for example, a suspect is known to visit a particular church every week, this item of data may be processed to the extent that this may be useful data for the detection of the criminal offence. Data on skin colour or ethnic background may also be processed as part of a description in cases in which the personal data and residence of the suspect concerned are not known. This Article forces the police officer to ask whether processing of certain sensitive data is unavoidable in a concrete case. Sensitive data may never be processed by way of an automatic action. In general, this means that statistical data on e.g. the relationship between ethnic origin and involvement in crime cannot be generated by means of recording the relevant data as part of the performance of police tasks. Such data may be obtained and processed, for example, in relation to specific cases in which it is clear, for instance on the basis of scientific research, that recording of the cultural or ethnic background is important for addressing certain problems. This may be an issue, for example, in problems such as honour killings or domestic violence. The way in which the police must be able to intervene may depend on the culture within which these problems arise. Statistical analyses are possible by means of an automated link between police data and population records, in such a way that the outcomes cannot be traced to persons.

Article 9
An important principle is that the processing of police data is linked to authorisation. The aim of this is to ensure that police data are only processed to the extent necessary for the performance of police tasks. Pursuant to Article 9, the person responsible is required to maintain a system of authorisation. Through the authorisation system, the person responsible is able to deliberately assign the processing of police data to the persons under his supervision and for whom the processing is necessary for the performance of their tasks, which are part of the police tasks. Within the standard of Article 9, the person responsible has a certain degree of freedom in the manner in which he designs the authorisation system. Particularly where the processing of data for the day-to-day police tasks is involved, the person responsible will have the necessary freedom regarding the way in which he assigns authorisation. Provision for the more specialised processes, in particular, will be made in further regulations concerning authorisation. The authorisation system to be co-designed by the person responsible must comply with the requirements of due care and proportionality. To the extent that employees within the police force need police data on an

incidental basis for the performance of their tasks, when they are not authorised to process that data, Article 18(1) requires that such data are made available.

Paragraph 1
The person responsible is required to observe the requirements of due care and proportionality in the development of the authorisation system. Among other things, these requirements entail that persons are not authorised more broadly than is necessary for the performance of their tasks. To that end, most authorisations will be linked to a particular position or functionality. In order to meet these requirements, the person responsible may, for example, make a distinction in the type of processing: the viewing, modification or provision of data. The form of the authorisation will depend partly on the risks associated with the tasks mandated to the officer concerned. The greater these risks, the higher the authority in the police organisation that must be authorised. By agreement with the police force, a national model could be developed for this if required, which could underlie the regulation in the national decree containing general measures. The granting of authorisation for the processing of police data, as provided for in Article 9(1), could, for example, concern the members of a detection team charged with an investigation. Within that team, distinctions are possible in terms of the nature of the processing. In accordance with the model of the procedures and rules for the processing of data that is currently in use in the police force, distinctions can be made by reading of all data, reading of all data and modifying one's own data, reading of all data and modifying all data and the removal of data.

Paragraph 2
The fact that police data may only be processed by police officers who are authorised for that purpose by the person responsible and only to the extent of their authorisation, makes it extremely important that the person responsible actually authorises the police officers to the extent that they are required to process police data in order to perform parts of the police tasks with which they are charged. Without such authorisation, they cannot process any police data. Paragraphs 2 and 3 therefore contain two closely related standards.

Paragraph 3
The person responsible enjoys a reasonable degree of freedom in the manner in which he designs the authorisation system. For example, it is conceivable that the person responsible will opt to authorise almost all police officers in his force to process police data with the aim of performance of the day-to-day police tasks. However, the person responsible may also opt to restrict the authorisation for certain positions to part of these data. In the authorisation for processing of police data, a strict limitation of the number of authorised persons is an obvious measure, in view of the requirements of due care and proportionality.

In view of the provisions of paragraph 2, it is important that the authorisation contains a clear description of the processes for which the relevant officer is authorised and the parts of the police task for the performance of which the processing is performed. The description in the authorisation serves firstly to provide clarity for the police officer concerning his powers with regard to the processing of police data. Secondly, the authorisation provides the manager with clarity concerning access to the police data that he must realise for the police officer concerned. Thirdly, in combination with the protocol obligation pursuant to Article 34, the authorisation forms the lead for the control and supervision provided for in Articles 35, 36 and 37. Through technical provisions, the person responsible can exercise adequate control, including after the event. For that purpose, filters could be installed or behavioural profiles could be used. The latter means that a user profile is drawn up for the officers involved in the processing of data. If discrepancies are observed between the user profile and the actual processing of data by the person concerned, this may form grounds for further investigation of the way in which the officer in question makes use of the police data.

Paragraph 4
In addition, persons who have not been appointed as police officer make a contribution to the detection of criminal offences. This could include persons who are occasionally hired by the police, for example because of their specific knowledge in a particular field, such as accountants, behavioural experts or psychologists. Authorisation must take place on the basis of each individual case, i.e. the authorisation will apply for a particular investigation. This can be developed by or pursuant to national decree containing general measures.

Paragraph 5
By or pursuant to national decree containing general measures, further rules shall be laid down pursuant to this paragraph, with regard to the categories of persons and the processing of data to which the authorisation may relate. In particular, this may involve the designation by further regulations of data processing that, due to its specialised character, must be restricted to persons specialised in that regard within the force, who, for example, meet certain training requirements. In particular, this then concerns the application of the search possibilities pursuant to Article 14 and the processing of police data on informants. The processing of the police data referred to in Article 15 shall be restricted by national decree containing general measures, to persons employed in the criminal intelligence service. This concerns persons who maintain contacts with the informant.

Article 10
In the draft, a choice was made to include a special confidentiality provision. The principle of the Article is that everyone is required to protect confidentiality if they gain access to police data concerning third parties. This applies not only for persons charged with processing police data or who obtain the data directly from the police, but also for any secondary and subsequent recipients to whom the data are passed on. They are also bound by the confidentiality obligation. This means that, barring the exceptions discussed below, the confidentiality obligation arising from this Article prohibits passing on of the data. A number of exceptions are made to the confidentiality obligation. Paragraph 1 provides that the confidentiality obligation does not apply for police officers to the extent that they are required to provide the data by or pursuant to a regulation laid down in the national ordinance, the provisions of paragraph 3 permit provision or the police task necessitates provision in exceptional cases. This latter phrase is explicitly intended for exceptional cases. Paragraph 2 creates an exception to the confidentiality obligation for recipients of the data, to the extent that this is required by a regulation laid down by or pursuant to the national ordinance or the need for this arises from their tasks.

Section 2. Processing of police data with a view to performance of police tasks

Article 11
This Article regulates the processing of personal data with a view to the performance of day-to-day police tasks. The performance of day-to-day police tasks is sometimes referred to as the 'eyes and ears' function of the police. This function covers all the parts of the police task referred to in Article 5 of the Police Kingdom Act of Curaçao, Sint Maarten, and of Bonaire, Sint Eustatius and Saba in a type of first-line variant. This is also referred to as the basic police work. The basic police work consists of surveillance, handling traffic problems, simple detection work, provision of assistance and enforcement of national ordinances and rules. The handling of traffic problems involves, for example, settlement of simple traffic offences, investigating traffic accidents and advising municipal authorities on traffic measures.
'Simple detection work' refers to the investigation of thefts and burglaries, securing tracks and recording burglary reports. Tasks that are not included in basic police care are detection work as referred to in Article 12, work for obtaining an insight, as referred to in Article 13, work as part of service provision, such as answering queries from citizens and handling requests for a police monitoring of suspects, service of documents, handling outstanding administrative decisions, etc. Keeping accounts concerning licensing, such as the assessment of licence applications, drawing up licensing regulations and central updating of records of these are not part of the day-to-day police tasks, but of the support tasks referred to in Article 16. The receipt of licence applications and, following the issue of licences, taking statements on infringements of licensing regulations are part of the day-to-day police tasks.

This Article also provides the legal basis for the processing of data concerning incidents of limited scale and duration, such as simple, brief detection inquiries, as long as no special detection tools are deployed in that regard and no detection team is formed. The data comes from the different parts of the police task, including, as referred to in this draft, upholding public order, maintenance of the legal order under criminal law, provision of assistance and the tasks for the judiciary.

Paragraph 1
For one year following the date of the initial processing, this data may be processed freely within the police force for the performance of day-to-day police tasks. This provision affords broad questioning possibilities in the context of 'basic police work'.
A broad circle of persons within the police force will be authorised for the processing of these data. Within this year, the police can use these data broadly to establish links between the different events that have occurred in that period. During this period, links can be made between the available data through automated comparison or the combination of items of data. However, both the gathering and the processing of data pursuant to this Article is bound by the general restrictions that apply for this pursuant to Article 3, such as the restriction that the processing must be necessary with a view to proper performance of police tasks and that it is relevant and not excessive in view of the purposes for which the data are processed.

Paragraph 2
On the basis of paragraph 2, in response to a concrete case, the hidden data 'can become available again for further processing if it appears from the system through comparison of data. A fairly broad circle of persons within the police force can also be authorised for the comparisons referred to in paragraph 2. This paragraph, too, once again explicitly provides that the processing in question must be necessary with a view to the performance of day-to-day police tasks. Viewing the data without a sound reason for this is not permitted. The term 'comparison' is more limited than the term 'processing'. The term 'comparison' means that data that were already available to the police officer concerned is compared with other data. This means that a comparison is made on a 'hit/no hit' basis. In the event of a hit, the police data for which further processing is regarded as necessary for the objective in question is processed further. Further search possibilities are not permitted where the legal provision refers to comparison. The categories of police data on the basis of which comparison is possible may be laid down by national decree containing general measures. This concerns the data needed in day-to-day police tasks in order to determine whether earlier processing has taken place with regard to the same person, the same vehicle or the same location. With this comparison method it is possible, for example, to search for older data if a suspect has admitted one or more criminal offences. If the seriousness and nature of the case do not justify a specific investigation in relation to Article 12, Article 11(2) affords the possibility of completing cases with police data processed earlier. The seriousness of an offence or the background of a person, such as his reoffending risk or background problems, is usually assessed partly on the basis of the historical data. This is particularly relevant in the case of the approach to frequent offenders. The possibility of comparing data is open to all police officers involved in the performance of day-to-day police tasks. The regime for processing of data, as developed in the first two paragraphs of this Article, also offers the possibility of data processing with a view to certain specialised tasks such as the settlement of international requests for legal assistance. This concerns tasks that do not imply specific processing of data within the meaning of Articles 12 and 13 or which fall within the support work referred to in Article 16 and that can therefore take place under the regime of that Article. If required, the person responsible can limit the circle of persons authorised to process the relevant data by means of authorisations.

Paragraph 3
The day-to-day police tasks include searches for links in order to assess on that basis whether there is cause to start an investigation, as referred to in Article 12 or an analysis, as referred to in Article 13. To that end, it is desirable that certain analyses can be conducted of the police data available 'behind the partition', which was processed with a view to the performance of day-to-day police tasks, other than by means of comparison. Pursuant to paragraph 3, a search for links between the data processed for the day-to-day police task can be conducted by means of combined search questions. Such processing may be at issue in tactical analyses, as part of which data are combined on breaches of standards that took place during a particular period or in a particular geographical area. In this way, crime involving frequent offenders can be identified, for example. The data made accessible on the basis of Article 16 may be involved in this. If files are then created with regard to frequent offenders who have been identified for the further approach to these persons, this involves specific processing within the meaning of Article 12 and Article 12-processing must be started. In practice, the analyses referred to here have usually already been made by the information desks.

Paragraph 4
The data that have (again) become available on the basis of the processing referred to in paragraphs 2 and 3 may be processed for the purposes of day-to-day police tasks, as referred to in paragraph 1. However, an obvious assumption is that in practice, there will be a need to include the data processed for the day-to-day police tasks in processing for other purposes within the police tasks. In the draft, such methods are referred to as 'further processing'. In paragraph 4, the possibility is offered of providing the data processed for the performance of the day-to-day police tasks for further processing for an investigation into the violation of the legal order in a specific case, processing on involvement in actions or criminal offences of a certain degree of severity or the reliability of an informant (Article 15). This makes it possible to start a specific investigation on the basis of data that have originated from the performance of day-to-day police tasks.

Paragraph 5
This paragraph provides that police data processed with a view to day-to-day police tasks must be destroyed within five years of the date of the initial processing. This term does not apply, therefore, for data that have been processed further, with the application of paragraph 4, for another purpose within the tasks of the police. For such data, the removal provision of the Article applies, on the basis of which the data are processed further, and the provisions of Article 17 then apply. To the extent that it is clear in advance with regard to certain data that have been processed in accordance with Article 11 that this is of exceptional importance for the performance of police tasks and therefore qualifies for longer-lasting processing, it is therefore obvious that it will be processed further pursuant to Article 12, 13 or 15. In view of the possibilities offered by the draft to further process data on the basis of Article 11 with a view to certain objectives within the police task on the basis of a different Article that provides for possibilities to process the data for a longer term, it would be disproportionate to keep all data acquired in relation to the day-to-day police tasks for longer than five years.

Article 12
If extra efforts are made to gather specific large amounts of data for an investigation aimed at enforcement of the legal order in a certain case, Article 12 provides the basis for the processing of police data. The term 'specific' relates to the processing of large volumes of structured data in relation to certain persons. Except in the case of criminal investigations, this will also be the case in fact-finding inquiries. Specific processing within the meaning of Article 12 in any event takes place as soon as detection inquiries are reported, a fact-finding investigation is started and as soon as special detection methods are deployed, such as systematic observation and bugging of telecommunications. After all, such cases involve extensive processing of data on persons whose precise involvement in the criminal offences to be investigated has yet to be established.
In practice, there will also be situations in which the time until the processing of data on the basis of Article 11 can take place and the time at which an Article 12 investigation must be started cannot be very sharply defined. In these cases, which do not clearly involve specific processing within the meaning of Article 12, there may nevertheless be cause to start an Article 12 investigation for other reasons, for example if search possibilities afforded by Article 12 are needed, if the longer processing terms provided by Article 12 are considered desirable or if there is a desire to process data hidden from other police data. Through the system of authorisation, it is possible to prevent data becoming accessible to persons who are not part of the circle of persons forming part of the investigation team.

Paragraph 1
The first paragraph of Article 12 provides that the police may process specific police data on persons for an investigation in a certain case. A case may be described as a time-limited incident or situation or as a series of incidents. It may involve a criminal investigation, for example because a murder has been committed, a fact-finding investigation, for example because frequent drug crime is identified in a particular area, or addressing public nuisance at a school or coffee shop. If files are produced regarding frequent offenders who have been identified in relation to Article 11, for the further approach to such persons, specific processing as referred to in Article 12 will often be involved. After all, data relating to such persons is then brought together on a large scale.
The issue in these cases is that the police, in response to a time-limited incident or situation or a series of incidents, gathers specific and extensive data on persons with the aim of restoring the rule

of law in that case or preventing a serious disruption of this. It can be noted in this regard that specific investigations that involve aspects of assistance (addressing youth crime, missing persons) are often not raised unless they also relate to the enforcement of the rule of law. The distinction between law enforcement under criminal law and provision of assistance is often not unambiguous. The search for a missing person, for example, who is known to have mental problems, may also relate to crime. To the extent that a specific investigation is not at issue, police data can be processed for the purpose of assistance on the basis of Article 11.
In processing on the basis of Article 12, no restrictions apply with regard to the status of the persons (suspected, unsuspected or not suspected); the police may gather everything provided that the personal data are of importance for the investigation. The circle of persons who have access to the data is regulated by means of authorisation. Through the authorisations, the data can be protected in both functional and geographical terms. This also serves the tactical hiding of the data within the police organisation. Article 12 regulates that the person responsible should authorise all detectives for whom this is necessary for the proper performance of their tasks to process the relevant data when this involves detectives of their own force. The regulation in this Article therefore provides for the possibility that, where investigations are conducted and specific personal data are gathered in response to a particular incident or situation, these data are processed to the extent necessary for the purpose of the investigation. However, the scale and scope of the data processing is limited by the purpose-specification and the principles of proportionality and legitimacy laid down in Article 3. Finally, as a result of the purpose-specification, the processing of the data must not have a permanent character and must be time-limited.

Paragraph 2
The purpose of the investigation must be recorded in writing, for control of compliance with the restrictions imposed on the processing of data by the principle of purpose-specification. To that end, the privacy officer maintains an overview of all current investigations and the purposes of the investigations that are opened in observance of this Article.

Paragraph 3
This paragraph clarifies that the data processed with a view to a particular investigation can be made available for further processing by the police officer responsible for this, for certain other purposes within the police tasks. The data may then be processed further for another investigation with a view to enforcement of the legal order in a specific case, as referred to in paragraph 1, for processing as referred to in Articles 13 or 15 or for the day-to-day police tasks. The possibility of providing data from an investigation for the purposes of another investigation is new in relation to the current legislation. This may concern data that is processed in relation to an investigation and regarding which the authorised officer suspects that it could be of importance for another investigation. This is the case, for example, if a witness in one investigation makes a statement that is relevant to the investigation into a murder of the operator of a petrol station, which is the subject of another investigation. In such cases, this paragraph provides grounds for the provision of the data for the other investigation. The use of the term 'provision' refers to the fact that the processing of the data takes place as a form of 'one-way traffic'; it is not permissible pursuant to this Article to examine, from a particular investigation or from a criminal intelligence unit, the extent to which useful data are available elsewhere within the police organisation (within certain investigations). Article 14 must be applied for that purpose. The possibility of providing police data that are processed as part of an investigation for the performance of day-to-day police tasks is also new. This may be at issue if the investigation team comes into contact with data on a frequent offender that may be relevant to their colleagues employed for the performance of day-to-day police tasks. Such data can then be processed further under the regime of Article 11.

Paragraph 4
This paragraph requires the removal of the police data if these are no longer necessary for the purpose for which it was acquired. After the objective has been achieved, the need for further processing of the data is no longer present. In the case of a criminal investigation that has led to prosecution, the situation in which the data processed pursuant to paragraph 1 is no longer necessary for the purpose of the investigation will not arise until the court has handed down a final decision in the case. After all, until that time the data will still be necessary if the public prosecutor, the examining judge or the judge at the hearing require further investigation. If the case is not solved and consequently, has not been submitted to the Department of Public Prosecutions, the

investigation will often be continued, but on a less intensive level. In that case, the data may remain necessary in the further investigation or if the team is reformed due to new leads. The data then usually remain necessary for the purpose of the investigation until, at the latest, the time at which the facts at which the investigation is directed are voided by prescription. Pursuant to the provisions of Article 4 it can also be reasonably assumed that the data gathered will be cleared at set times and/or at a number of decisive moments in the process and that part of this will be destroyed due to the fact that, according to a reasonable assessment, it will no longer be of importance for the purposes of the investigation. An example of such a decisive moment is the submission of the official report to the Department of Public Prosecutions; at that moment, which of the investigated facts may require further investigation during the criminal proceedings will be clear. The data concerning other facts can therefore be deleted unless they are still necessary for another investigation. Article 12(4) makes provision for this.

Article 13
Like Article 12, Article 13 concerns specific and extensive processing of data on persons by the police. This concerns processing of data in order to obtain an insight into the involvement of certain persons in certain serious criminal offences or in actions that could indicate the plotting or committing of certain categories of criminal offences that give rise to serious threats to the legal order or in actions that constitute a serious disturbance of public order. In contrast to Article 12, the focus here is not so much the incident or the situation as the structure of the information position. This Article provides for the more permanent forms of data processing. This more permanent processing of data is necessary in connection with the nature of the criminal offences or actions at issue, as raised below in the memorandum on paragraph 1. A good information position is essential in order to address the relevant threats to the legal order effectively. In contrast to Article 12, the categories of persons concerning whom data can be processed are bounded by law in Article 13. The persons must be involved in facts or actions that require the permanent attention of the police. The processing of the data has a proactive function, in order to obtain a good information position. This data position may lead to a decision to start an operational criminal investigation (on the basis of Article 12) or to take operational measures in relation to public order. This processing, too, is performed only by police officers authorised for that purpose by the person responsible. With regard to paragraph 1(a), this is primarily expected to be the employees of the criminal intelligence unit who are charged with maintaining contacts with informants, but may also concern crime analysts or other police officers.

Paragraph 1
Paragraph 1 of this Article offers the possibility of processing police data with a view to obtaining an insight into the involvement of certain persons in certain serious criminal offences or in actions that could indicate the plotting or committing of certain categories of criminal offences that give rise to a serious violation of the legal order or actions that constitute a serious disruption of public order. The reason for processing of data pursuant to Article 13(1) may be, for example, that analyses conducted pursuant to Article 11(3) reveal a long-lasting pattern of drug trafficking in a particular district. If further insight is needed into the involvement of certain persons in the preparation or committing of offences relating to drug trafficking, processing may be commenced pursuant to Article 13. If that processing provides enough leads for a concrete criminal investigation, the data from that investigation may be processed under the regime of Article 13. The processing pursuant to Article 13 may also provide data that should be widely available within the police force for the performance of the day-to-day police tasks. An example of such data is that a certain person is armed and dangerous. The relevant data can then be made available for further processing for day-to-day police tasks. The further processing of the data will then take place under the regime of Article 12. Sub-paragraph b of this paragraph concerns the processing of data in order to obtain an insight into the involvement of persons in actions that could indicate the plotting or committing of criminal offences that, through their scale or severity, or their relationship with other criminal offences, represent a serious risk for the legal order. Addressing these criminal offences requires the development and maintenance of a permanent information position. This section concerns serious criminal matters such as terrorism, that represent a major threat to society and regarding which the conventional criminal law approach, which assumes that the government will respond to violations of standards, is not sufficient. In order to be able to address these threats and to obtain an insight into the circle of persons who, on the basis of the actions that they perform, may be involved in this, it is necessary to gather and analyse relevant data so that the violation of

standards, such as a bomb attack, can be prevented. The reason for the processing of data is that the actions may indicate the plotting or committing of certain categories of criminal offences that give rise to a serious threat to the legal order. The categories of criminal offences that seriously threaten the legal order, regarding which data may be processed on the grounds of this section, shall be described by national decree containing general measures. Only data concerning involvement in actions that could indicate the plotting or committing of these offences may be processed. The designation by national decree containing general measures, prevents excessively broad processing of data on actions and on the persons involved in these.

Paragraph 3
Processing of data on a broader circle of persons is required in order to build up an information position on actions that could indicate the plotting or committing of certain categories of criminal offences that give rise to a serious threat to the legal order. In order to identify persons involved in such actions effectively, it is necessary to gather data at a very early stage. For that reason, this paragraph provides that personal data on persons involved in the actions referred to in paragraph 1(b) may be gathered and stored. These indications may lie in the membership of certain associations, such as gun clubs, membership of groups that are less accessible to the government or visiting certain websites on the internet. Pursuant to the provisions of section 5, good control of this processing of data can be exercised through the internal and external forms of supervision.

Paragraph 5
This paragraph states that an authorised officer may provide the data encountered as part of the processing of data pursuant to paragraph 1 for further processing in a current investigation or an investigation still to be opened on the grounds of Article 12, processing on the grounds of Article 15 or for the performance of day-to-day police tasks, as referred to in Article 11. In the processing of data pursuant to paragraph 1(b), persons concerning whom there are reasonable suspicions of involvement in the plotting or committing of the criminal offences referred to in paragraph 1(a) can be identified. Persons can also be identified as suspects. In such a case, the data can be further processed by the criminal intelligence service or under the regime of Article 12. A similar working method applies for the regional intelligence service, because the regional intelligence service may encounter data that is important for the detection of criminal offences. By means of a procès-verbal, this data can also be made available for further analysis by the criminal intelligence service. In the cases in which the relevance of data to an investigation is evident, the criminal intelligence service can also pass on the data directly to the relevant investigation. It is also possible that the data processed in the context of this Article is relevant for the performance of day-to-day police tasks. For example where this involves intelligence from an informant concerning potential disruptions of public order at a particular location. In such cases, this intelligence may be provided for further processing under the regime of Article 11, so that surveillance can be intensified at the location in question. Naturally, there may be reasons to provide the data in such a way that the identity of the informant cannot be traced or that data that should not be widely available within the police force is released in other ways.

Paragraph 6
This paragraph provides that data will be removed as soon as it is no longer necessary for the purpose of the processing. For the data processed on the basis of Article 13, it is important to note that data are cleaned every six months, with data that are no longer necessary for the purpose being removed. This paragraph contains the obligation to do so. As there is no natural limit for the Article 13-processing through the closure of an investigation, this paragraph provides that the data will be removed no later than five years after the date of the latest recording of data that shows the need for the processing of the personal data of the person concerned with a view to the objective referred to in paragraph 1.

Article 14
This Article offers the possibility of comparing police data automatically, on the basis of an investigation or processing as referred to in Article 12 or 13, or of processing it in combination with other police data, in order to determine whether links exist between the items of police data in question. The data can be viewed, to the extent that this is necessary for an investigation as referred to in Article 12(1), or for processing as referred to in Article 13(1). It has already been

stated in the General section of this Explanatory Memorandum that, in view of the risks for the protection of personal privacy and the hiding of sensitive investigations, it is necessary to bind such processing of criminal police data by strict criteria. Persons who originally appear in a particular capacity in individual investigations (as a suspect, witness, victim or in another capacity) may be shown in a different capacity (as a suspect) on the basis of this process. In this way, data obtained in one investigation through the application of far-reaching powers, such as the seizure of accounts, may become available to another investigation that, in itself, could not have provided grounds for the seizure. It must also be borne in mind here that the data that is processed in relation to Articles 12 and 13 has not or cannot always be tested for accuracy and completeness. This may also involve 'bulk data', data obtained through telephone taps and the seizure of computer data, before the data relevant to the investigation have been selected. Such bulk data may include data on citizens who are not under suspicion. In view of the character of this form of data processing, which can be far-reaching in relation to personal privacy, the person responsible or the police officer concerned – and in the case of paragraph 4, also the competent authority – must carefully consider the interests served by viewing other investigative data in the light of the interests of the persons whose data could be involved in this investigation. The principles of proportionality and subsidiarity must be observed here, among other things. Obviously, no data may be included in the comparison of data that should have been destroyed pursuant to this national ordinance or to the Code of Criminal Procedure. Reference must also be made in that regard to the additional requirements laid down in the Code of Criminal Procedure regarding the use of certain data for other purposes within the police task.

Paragraph 1
This paragraph provides for the possibility of automated comparison of police data from the investigation in question with police data processed in another investigation pursuant to Article 12 or for the performance of day-to-day police tasks pursuant to Article 11. In view of the potentially far-reaching character of this form of data processing, a number of criteria apply. Firstly, the comparison of the data must be based on clear grounds. The comparison of data in question must be necessary for the investigation of which the data is viewed. The requirements of proportionality and subsidiarity must be observed here. Secondly, the comparison of data is more limited than the processing of data and this ensures that the viewing of other data takes place only on the basis of data already obtained in the investigation from which the data is requested. This therefore is about verification. The comparison of data takes place on a 'hit/no hit' basis. Thirdly, the comparison of data is permitted only by officers who are authorised for that purpose. The circle of police officers who are permitted to view the relevant data is therefore confined to those who should view it on the basis of their tasks. Further rules may be laid down for this by national decree containing general measures, pursuant to Article 9(5). Fourthly, the further processing of the equivalent data is made dependent on the consent of an official authorised for that purpose. This officer must consider the extent to which further processing of the relevant police data for another investigation is justified, in view of the interests of proportionality, subsidiarity and hiding at stake. Pursuant to Article 6(6), the person responsible is required to designate such an official. This could be the head of the criminal investigation department or the leader of the relevant investigation team. The comparison of data pursuant to this paragraph does not extend to the data processed pursuant to Article 13. The viewing of police data on the persons concerning whom data are processed under the regime of that Article could easily lead to the circulation of sensitive investigation data that are processed by the relevant criminal intelligence service, such as on informants who have provided data on the modus operandi of a dangerous criminal. In view of the interests concerned, a decision was made not to involve the data processed pursuant to Article 13 of this draft in the comparison of data of paragraph 1.

Paragraph 2
This paragraph provides for the possibility of automated comparison of police data that is processed for a purpose referred to in Article 13 with police data processed in an investigation on the grounds of Article 9, a purpose other than those of Article 13 or for the performance of day-to-day police tasks pursuant to Article 11. In view of the analysis of criminal intelligence, it may be important to view data processed for a different purpose on the grounds of Article 10, an investigation on the grounds of Article 12 or for performance of day-to-day police tasks pursuant to Article 11. On the basis of this paragraph, a search of more data can be conducted than on the basis of paragraph 1, because the data of Article 13 may also be involved.

Paragraph 3
This paragraph regulates that further rules may be laid down by or pursuant to a national decree containing general measures, with regard to the method of performing the comparison of data. This may relate to the categories of data on the basis of which comparisons can be made, the encoding of data and the way in which the links are made visible.
The principle of the draft is that police data are provided to police officers to the extent that they need this for the performance of their tasks. However, there may be serious reasons to refuse the provision of police data. A regulation for this is included in Article 18. In these cases, there may also be reasons to exclude the relevant police data from the establishing of links pursuant to Article 14, so that the relevant data cannot become known in that way outside the circle of police officers involved in the investigation. It is technically possible to design an automated system in such a way that restrictions are imposed on the circulation of data. This could include data concerning which provision to other parties could create risks for the health or safety or informants or witnesses. This can be realised, for example, by 'earmarking' or encoding data so that it can be accessed only by a restricted circle of persons.

Paragraph 4
Paragraph 4 provides for the possibility of combined processing of police data in the interests of an investigation as referred to in Article 12 or for an objective as referred to in Article 13. Once again, access to the data must be necessary for the investigation or for the analysis. The search method, however, is broader than in paragraphs 1 and 2, because it is not restricted to comparison. In this way, all data can be viewed. As already noted in the General section, the necessity criterion is developed in more detail in the Strasbourg jurisprudence with the requirements of the presence of a 'pressing social need' and of proportionality and subsidiarity. The pressing social need may be at issue in various cases, such as the prevention or detection of a serious criminal offence that could lead directly to serious disruption of society and that cannot be prevented or solved by other means. This could involve an attack on infrastructural work where many people come together, a kidnapping, hostage-taking or a series of serious criminal offences where there is a need to combine all relevant data on certain persons, including all data processed in relation to Article 13. This possibility may also be at issue in the case of terrorist action, or the threat of this. It could also include situations in which there is a need for the analysis of data when there is no concrete suspect or suspicion, such as a situation in which relationships between attacks conducted at different locations in the country are at issue. These relationships can become identifiable through analysis based on certain profiles of offenders, victims or facts. The serious threat to the legal order involved in the relevant case justifies the combination or searching of all available police data for the detection of these criminal offences. Finally, this could include tactical analyses in relation to which data concerning violations of standards that took place in a particular period in a particular geographical area is combined on the basis of composite search questions.
On the basis of the outcomes of the investigation, a decision may be made to conduct a criminal investigation directed at one or more persons. The processing of the data relating to such a criminal investigation could take place under the regime of Article 12 if there is specific processing of data on persons. Due to the breach of the principle of purpose-specification that underlies the regulation of Articles 11, 12 and 13, the potential breach of the personal privacy of the persons concerned and the consequences for the hiding of sensitive data within the police force, such a broad processing possibility must be bound by strict criteria. The principles laid down in Article 3 play an important role in this. Only in very serious cases can processing pursuant to paragraph 4 comply with the requirements of necessity, as developed in the Strasbourg jurisprudence, and of proportionality. This is reflected in the text of the draft in the words 'in exceptional cases' and the requirement that the competent authority issues instructions for this. The realisation of the further restriction on the basis of a substantive criterion, such as the criterion that such processing is permitted only in the case of a serious violation of the legal order or a threat to this, was considered. However, there are objections to the use of such a substantive criterion. Firstly because such a criterion could prove to be too restrictive in practice as soon as a need exists to apply this search possibility in cases in which the serious violation of the legal order is not evident. Furthermore, this criterion assumes an assessment: due to the interests at stake and the nature of the consideration of interests, assessment by a holder of authority is then an obvious step. Furthermore, the circle of persons who can be authorised to perform such an analysis must be very restricted. Within the force, only a few

police officers who have the required experience could be authorised for this. Pursuant to Article 9(6), further rules will be laid down in this regard by national decree containing general measures.

Article 15
This Article provides for a regulation for data processing concerning informants. It concerns data regarding the actions of informants and integrated reports on meetings conducted with the informants. The data in the register of informants is protected and does not serve for operational use. The criminal intelligence provided by an informant may also be recorded in other police registers, to the extent that this data complies with the description of their purpose. This means that after the data has been recorded in the register of informants, the desirability of further processing with a view to an investigation as referred to in Article 12 or an analysis as referred to in Article 13 is assessed.

Paragraph 1
Paragraph 1 describes the purpose of the processing. The purpose of registration is to maintain a full picture of what happened in relation to the person of the (permanent) informant. This total overview is necessary for the control, management and quality assessment of the informant, as well as for the assessment of the use of data in relation to the risk factor for the informant and ultimately, for the accounting for and use of data provided by the informant. The processing of data on the basis of Article 15 relates to all observations, agreements and findings in relation to the informant, the person of the informant and the data provided. This includes reports of meetings describing the content of the conversations conducted with the informant, relevant data on antecedents and any involvement in criminal investigations, the day-to-day conduct of the informant and the contacts that he maintains with persons who may be involved in criminal offences. Such processing of data is necessary firstly for the smooth progress of contacts with the informant. On the basis of the data, the runners can form a view of the background and conduct of the informant and of the agreements reached with him at an earlier stage. In addition, the processing of the data serves as a basis for the processing of data by the criminal intelligence unit. This concerns the 'gross data' that can give rise to the provision of data to the criminal intelligence unit with a view to further refinement of that data. This 'net data' can be exchanged with the criminal intelligence units of the other regional forces. However, a term is attached to this, as included in paragraph 2. The purpose-specification of this paragraph also includes account for the use of the data in criminal proceedings. In that case, the storage term of paragraph 6 applies.

Pursuant to Article 9(6), the circle of persons who can be authorised to process data on informants will be further restricted. In view of the sensitivity of such data, authorisation must be restricted to certain police officers employed at the criminal intelligence service. Access to the 'informant codes' must be very strictly limited, for example to the head of the criminal intelligence service or his deputy.

Paragraph 2
The data that the informant provides should be kept in order to enable the assessment, on the basis of the overall picture presented by the data, of whether the data can be used in view of the safety of the informant. It is also necessary to assess the extent to which data qualify for operational processing, i.e. for involvement in an investigation pursuant to Article 12 or processing as referred to in Article 13. Paragraph 2 makes further processing possible within a period of four months after the date of the initial processing. If no term were set then, due to the fact that the data processing has a broad character, processing with a view to the assessment of the reliability of the informant could evolve in practice into operational processing that is aimed partly at the analysis of data with a view to the objectives of Article 13. This is undesirable, as it would undermine the own regime geared to this, of Article 13.

Paragraph 3
For the explanation of this paragraph, reference is made to the explanation for Article 13(2). In addition, it can be noted that the specific objective of processing may mean that data are gathered on persons concerning whom informants provide data and persons with whom the informant maintains contacts in daily life, such as family members or acquaintances, to the extent that this is necessary for control and management of the informant.

Paragraph 4
For the acquisition of a clear picture of the informant's contacts and conduct, and thus for an accurate assessment of the risks associated with the deployment of that informant, it is essential that all available data on that informant within the police force can be processed. Pursuant to Article 16(4), it is possible to determine whether the informant is involved in certain investigations or other processing. This system is described in the relevant explanation. In addition, this paragraph offers the possibility of direct searches for police data on the informant. Direct comparison of data may be at issue in cases where data are sought that has not been made available pursuant to Article 16. In contrast to the comparison of data pursuant to Article 14, no additional consent is required for the further processing of the data from an official authorised for that purpose. The need to hide processing of data on informants prevents this. The data are processed solely with a view to the control and management of an informant and will not be made available for further processing pursuant to Article 11, 12 or 13. Equally, the data processed on informants cannot be involved in the establishment of links between data pursuant to Article 14. Due to the sensitivity of this data, no reference to Article 15 is included in Article 14.

Paragraph 5
Pursuant to paragraph 1, police data can be processed with a view to the control and management of an informant as well as the assessment of and accounting for the use of data from informants. This not only concerns data such as the name and address, but also data on the daily life habits of these persons and the way in which supervision of their safety is conducted. The recorded data are not used to investigate criminal offences but for the management and control of these persons. Due to the sensitivity of the recorded data, the risk that unrestricted use of such data can cause for the safety of the person concerned and thus the need to be able to hide this also within the police organisation itself, this paragraph provides for the possibility of applying the regime of this Article to the processing of police data concerning e.g. infiltrators or witnesses included in a witness protection programme. The categories of persons concerning whom this possibility may be used can be designated by national decree containing general measures. The categories of persons concerning whom police data are processed are also designated here, because the application of paragraph 3 will not be a good match with the processing of data on infiltrators or witnesses.

Paragraph 6
This paragraph provides that data will be destroyed no later than ten years after the date of the latest recording of data showing the need to process the personal data of the person concerned in view of the objective referred to in paragraph 1. If the registered informant has not given any reason to process data during this period, therefore, the data must be destroyed. The background to this provision lies in the fact that the processing of data pursuant to paragraph 1 can take place with a view to different objectives. If the police data originating from the informant is processed further, the processing term is determined by the operational use of that data. This means that the processing terms applying for the processing of data under the regime of the relevant Articles is leading in the determination of the processing term for that data. The processing term for the police data processed with a view to the control and management of the informant is linked to this through the reference to the purpose referred to in paragraph 1. The term for saving data in this paragraph applies for all police data processed pursuant to paragraph 1. At the end of ten years following the last processing of data showing the need to process the personal data of the person concerned with a view to the objective referred to in paragraph 1, the data must be destroyed. This term sets a clear limit on the use of the data, but at the same time provides the necessary scope for processing of the data for accounting for its use – for example on the basis of criminal proceedings – or the ability to track the informant in relation to the assessment of his reliability. At the end of ten years, the data must be destroyed unless reasons arise within that term for the processing of police data with a view to the objective of paragraph 1. Finally, it should be noted that paragraph 2 entails that part of the data provided by the informant may fall under different regimes for the processing of police data, so that certain data may be saved and processed with a view to different objectives during the term that applies for the processing of the item of data for the relevant purpose within the police task.

Paragraph 7
The main features of the definition of an informant are that the informant provides data on persons involved in criminal offences that have been or are to be committed, that the informant himself is

not involved in committing criminal offences and that the provision of the data gives rise to risks for the informant or for third parties.

Article 16
This Article provides for a regulation for further processing of personal data that were originally processed with a view to an objective as referred to in Article 11, 12 or 13, to support the police task. On the one hand, Article 16 provides for an additional legal ground for the further processing of data for purposes other than those for which they were already processed. The additional legal ground relates to supporting tasks. On the other hand, this development of Article 16 provides for a further development of the obligation that already exists pursuant to Article 18, to provide data relevant to another person responsible to that person. Article 16 has a tiered character in terms of levels of hiding. The data that can be made available for viewing nationally requires no special hiding within the police task. The relatively innocent character of the data justifies the fact that in principle, it may be processed further for all parts of the police task. In accordance with the principle of Article 18(1), the data provided in this way may in principle be used only for the purpose for which they are provided in the relevant case. Via the written record, the person responsible states in advance which items of the data are made directly accessible and which are provided to other forces, to the extent necessary to support the police task, and for which purpose. Secondly, the data provided pursuant to paragraph 2 requires stronger hiding. This hiding will primarily be expressed in the form of a more restricted category of authorised persons. Pursuant to Article 9 of the draft, rules for this will be laid down by national decree containing general measures. The fact that the data concerns specialised matters means that only persons authorised for these specialised matters will need the data for the performance of police tasks. Once again, an assessment takes place in each case and in principle, the data may only be used for the purpose for which it is provided, albeit that Article 18 also offers the possibility of providing the data for a different purpose within the police tasks, on the basis of a prior assessment in each case. To the extent that data are processed on the grounds of Article 16 in response to requests from other institutions, the requests to that end are first recorded pursuant to 11, 12 or 13, after which further processing may take place on the grounds of Article 16. With regard to requests for international legal assistance too, the initial processing will always take place in relation to Article 11, 12 or 13, after which further processing can take place pursuant to Article 15. The principle of the draft is that the person responsible supervises correct processing of data that takes place under his management. The person responsible in the force that processes the data further is then required to supervise compliance with Article 3 and to take measures as referred to in Article 4. That responsibility relates only to the processing of data that takes place under his responsibility. With regard to the data processed for the supporting tasks, the obligation laid down in Article 3(4) to report the source of the data and the way in which it was acquired does not apply. The reason for this is that part of the data processed for the supporting tasks originates from different sources, including from the set of data gathered for the performance of day-to-day police tasks. After all, this obligation does not apply for the processing of data for the performance of the police task either. However, it would be obvious for existing reports of the source of data and the way in which it was acquired to continue to accompany that data when it is processed further in relation to Article 16.

Paragraph 1
This paragraph provides the basis for further processing of certain data from Articles 11, 12, and 13 for purposes other than those for which the data was originally processed and to that end, to process it for longer. The person responsible determines which data qualify for further processing for the purposes referred to in paragraph 1 and whether they can be made available for viewing nationally or are made available on the basis of an assessment in each case. The person responsible must assess which data qualifies for further processing on the grounds of Article 16.

Paragraph 3
It is extremely important that there is a possibility to coordinate the different instances of processing within the police force. Firstly because this may be of importance for the further approach to a criminal investigation. Secondly because it is necessary to know the extent to which investigations are conducted within the police force into particular persons or locations, or other entities. The possibility of exchanging police data relating to a person concerning whom processing is performed on more than one occasion is essential for the effectiveness of the investigation of

criminal offences. Pursuant to this paragraph, links can be laid through automated comparison between the different instances of data processing that take place in relation to a particular person in the interests of different objectives within the police task.

Paragraph 4
In order to enable supervision and to provide for public access to information and foreseeability, an obligation has been included for the person responsible to record a number of aspects of the processing in writing. This will be developed further by national decree containing general measures. The processing terms depend on the specific objective for which the relevant data are processed. By national decree containing general measures, further rules will be laid down for this. A uniform regulation for saving all data covered by this Article is not feasible, due to the great diversity of the data.

Article 17
Article 17 aims to provide for limited periods during which removed police data are kept for the handling of complaints and accounting for actions. As a general rule, data that is processed pursuant to Articles 12 and 13 is removed as soon as it is no longer necessary for the purposes for which it was processed. Data that proves to be inaccurate is destroyed pursuant to Article 4. Data that are removed are no longer accessible for operational purposes but are not destroyed immediately. They are 'set aside', as it were. Through automation, this need only mean that they are made inaccessible. In exceptional cases, the data can be made available again for operational use.

Paragraph 1
Paragraph 1 describes the purposes for which police data are kept after their removal. Democratic control must also be possible after some time, for example in relation to the working method in the exercise of far-reaching powers. The data must then still be available. Pursuant to the draft, a term for keeping removed data is introduced and is set at a uniform period of five years for all data. This will lead to greater clarity and uniformity regarding the saving and destruction of police data.

Paragraph 2
As in principle, the saved data are no longer available for operational use, it is obvious that they should also not be provided to third parties. With the exception of Articles 24 and 25, the provisions of paragraph 3 are therefore declared inapplicable to these data. Otherwise, removed data could be restored through provision to third parties. This would not be consistent with the removed character of the data. However, the general provisions and the provisions concerning legal protection apply in full to saved data. Citizens have the right to view the data kept in relation to them and to ensure that these police data, too, are correct.

Paragraph 3
In this paragraph, an exception is formulated to the rules that removed data should no longer be available for operational purposes. First and foremost, the potential relevance for future investigations does not, in itself, form an argument for saving data. The purposes for which removed data are saved are described in paragraph 1. In exceptional cases, however, a situation may arise in which the data saved for the purposes described in paragraph 1 must be made available for operational purposes, for urgent reasons. If, for example, it becomes clear in the course of an investigation on the grounds of Article 12 that certain removed data could be exceptionally relevant for solving the case, and these data are still available in the category of removed data, it would be unreasonable if it was not permissible to retrieve these data. The purpose for which the retrieval of the data is necessary, and the data concerned, must be clear in advance however. Pursuant to this Article, undirected searches or processing in combination with new data are not permissible.
In order to prevent excessively easy deployment of this facility, an order from the competent authority is required. The task of the competent authority is to assess whether an exceptional case is indeed involved and whether it is sufficiently clear in advance which data are involved, so that no undirected search actions need take place in the data that have been removed.

Paragraph 4

This draft includes a regulation concerning the removal, saving and destruction of data. After all, with a view to the principles of necessity, purpose-specification and protection of the privacy of citizens, an exhaustive regulation is laid down for the processing of police data. However, paragraph 4 includes the possibility of meeting exceptional interests of cultural preservation, in the form of a hardship clause. Pursuant to this paragraph, it is possible to prevent destruction of police data, to the extent that, in the view of the person responsible, this is counter to the value of the archive files as elements of the cultural heritage or for the purpose of historical research.

Article 18

Paragraph 1
Paragraph 2 of the draft formulates a number of objectives within the police task. Police officers can process data in view of those objectives. In a number of cases, such processing is subject to authorisation by the person responsible under whose management the processing takes place. The broad definition of the term 'processing' means that other police officers may be involved, within the objective of the processing. It is possible, for example, that police officers responsible for surveillance may further process certain police data on a frequent offender with a view to the performance of day-to-day police tasks. Such data may also be of importance for other police officers who come into contact with the relevant person as part of the performance of day-to-day police tasks. The viewing and if necessary, further use of this data may also fall under the processing of police data for the original purpose. Such a form of further processing is at issue in Article 11(2) and 11(3). In addition, paragraph 2 provides for the possibility of further processing of police data with a view to a different objective within the police task. For example if police data have been gathered on a particular person with a view to the performance of day-to-day police tasks but, because that person is also suspected of serious criminal offences which are under investigation by an investigation team, also prove to be important for that investigation. Such a form of further processing is at issue in Articles 12(3) and 13(4). The draft provides for the possibility that certain categories of police data from the investigation are compared with other police data that are already available. This is regulated in Articles 14(1), 14(2) 15(4) and 16(4).

This paragraph provides for an obligation for the person responsible to make police data available for further processing, as described above. This obligation relates to both the persons under his management and the persons under the management of another responsible person, to the extent that they need the data for the performance of police tasks. As part of the performance of his tasks, a police officer may come into contact with the different persons responsible, either because he needs data that are processed by a different police force or because the processing of data with a view to a particular objective may take place under the direction of different persons responsible. The person responsible is required to provide data, to the extent that these are necessary in view of the performance of the police task in accordance with the rules of paragraph 2 of the draft. Viewing and any further use of that data takes place under the responsibility of the person responsible under whose management further processing then takes place. This also means that further processing by the police officers under the authority of another person responsible is justified only if, in the cases in which authorisation is required, these officers are authorised for that purpose by the person responsible. Developments in data technology make it possible to provide police data electronically, the transfer of police data without human intervention will then become the rule rather than the exception. Taking account of the technological developments, the person responsible may opt to provide the police data electronically, directly to police officers who fall under the management of another person responsible.

Paragraph 2
This paragraph offers the possibility of refusing to provide data to a police officer from the person responsible's own force or to provide police data to a police officer under the management of another person responsible in the cases in which there is reason to do so for technical investigative reasons. In the cases of sensitive criminal investigations with a high termination risk, there may be a need to protect data, including within the person responsible's own police organisation. Such investigations are also referred to as 'embargo investigations'. The investigation into a particular incident could be harmed because data are provided to police officers who are not directly involved in this investigation. The phrase 'in exceptional cases' shows that such a method must not be allowed to become a general line of conduct in practice, but is only permissible as an exception. The

main point of the legal regulation is that data are provided to other police officers to the extent that they need this for the performance of police tasks, either directly or through processing with a view to supporting tasks, as referred to in Article 16, unless there are sound reasons not to do so. The draft aims to offer the police greater scope for the exchange of data and broad application of this provision could seriously harm that principle. This principle will be reflected in the further rules to be laid down by national decree containing general measures. In the cases described above, there may also be reasons to exclude the relevant police data from the establishing of links pursuant to Article 14, so that the relevant data cannot become known in that way outside the circle of police officers involved in the investigation. To that end, Article 14(3) includes the possibility of laying down rules on the encoding of police data by or pursuant to national decree containing general measures, by assigning an indication to that data concerning its reliability and confidentiality and the possibility of processing it further for an analysis or investigation.

Article 19
This Article regulates the provision of police data to members of the Department of Public Prosecutions with a view to certain objectives or for the performance of certain tasks.

Article 20

Paragraph 1
If a legal regulation concerning intelligence services provides for this, police data may be issued to that intelligence service.

Paragraph 2
The reference to assistance for an international criminal court applies as a mirror provision for Article 6 of the International Criminal Court Implementing Act of 20 June 2002, which offers the possibility of providing data to the Court if this is necessary for the proper performance of the tasks of the Court.

Paragraph 3
The provision of police data to the police authorities of other countries is bound by the general condition that such provision is necessary for the performance of the police task in the Netherlands or in the relevant country. This is consistent with the necessity principle of Article 3(1) of the draft. Reference is made to Article 39(4) and 39(5) of the Police Kingdom Act of Curaçao, of Sint Maarten, and of Bonaire, Sint Eustatius and Saba. Pursuant to these paragraphs, there is an obligation to exchange police data between the police and the European section of the Kingdom and the police of Curaçao and Sint Maarten. Article 59 of this Kingdom Act provides for the possibility of arranging for Article 39(4) and 39(5) to enter into force later than the rest of the Kingdom Act. These paragraphs will enter into force as soon as this national ordinance and the equivalent regulation on Sint Maarten enter into force. Until these paragraphs enter into force, an exchange is possible on the grounds of the mutual arrangement pursuant to Article 57 of the Kingdom Act.

Paragraph 4
The provision of data to other countries is bound by the criterion that sufficient assurances are present at the recipient institution for the correct use of the data provided and for the protection of personal privacy. Countries that are members of the Council of Europe can be expected to comply with this criterion. For countries where this is not the case, an assessment must be made in each individual case as to whether the provision of the data is justified in view of the nature of the data and the purpose for which they are requested, taking account of what is generally known about the relevant country.

Paragraph 5
Further rules on the provision of data to foreign police authorities or international investigation organisations shall be laid down in a national decree containing general measures.

Article 21
The persons to whom and the institutions to which data shall or may be provided can be designated by or pursuant to national decree containing general measures. This concerns persons and institutions that require certain police data on a structural basis for the proper performance of their

tasks. It also concerns persons and institutions with a national task. Pursuant to Article 21, these institutions may be designated if there is a serious general interest that necessitates the provision of police data. The criterion of a serious general interest is drawn from Article 8(4) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ of 24 October 1995, L 281). In view of Article 8(2) of the European Convention on Human Rights (ECHR), the term 'serious general interest' must be deemed to refer to the interests of the country's national security, public security or economic welfare, the prevention of disorder and crime, the protection of health or good morals or the protection of the rights and freedoms of other parties. Processing of data serves a general interest if that processing is of importance for the society. From the point of view of a serious general interest, processing of data is justified if these data are of more than ordinary significance for the society. Application of the criterion of the serious general interest implies a consideration of interests. The interest served by the provision of data is assessed in terms of the interest of the personal privacy of the persons to whom the police data relate. The principles of proportionality and subsidiarity must also be taken into account in this consideration of interests.
The designation of persons and institutions may take place by or pursuant to national decree containing general measures. This provides the possibility of designating the persons or institutions concerned by means of a ministerial regulation. Further restriction of the categories of persons and the categories of data to be provided is reserved for a national decree containing general measures.

Paragraph 2
Paragraph 2 grants the Minister of Justice the authority to derogate from any regulation concerning the provision of police data. This authority concerns all provision regulations of this section and may lead to both the granting of consent to provide data and the imposition on the person responsible of an obligation to do so. The proposed derogation authority may be used only in exceptional cases, and a categorical derogation is therefore not possible. The minister must always state in his order the data for which he permits derogation from the provisions of this section.

Article 22
This Article offers the possibility of providing police data in exceptional cases. Under certain conditions, the person responsible may decide to provide police data to third parties. A number of requirements apply. Firstly, provision is only possible for certain purposes, i.e. the prevention and investigation of criminal offences, the maintenance of public order, the provision of assistance to those who need it or the performance of supervision of compliance with regulations. These objectives may entail that police data are provided to third parties. The formulation of the objectives in sub-paragraphs a, b and c is consistent with the description of the police task in Article 5 of the Kingdom Act. This means that data can be provided to third parties, such as other government services or non-government institutions if this is consistent or compatible with the objectives for which the police themselves process the data. Provision pursuant to Article 22 may include the provision of police data to a victim or to the party who represents the interests of the victim in law with a view to a claim by the victim for compensation for the damages he suffered. There may be reasons for such provision to the extent that this involves data that are not available to the Department of Public Prosecutions, for example because no official report has been taken or because the official report was not submitted to the Department of Public Prosecutions. The purpose of the provision in that case is to provide assistance to those who need it (Article 22(c)). Another example concerns the provision of data on a child who is a victim of abuse to the management of a school or to the teacher concerned for the provision of assistance to the child in question. This may also concern the provision of police data to municipal authorities for supervision of compliance with brothel licences, to the extent that such provision does not take place in relation to Article 23. Secondly, the provision must be necessary in view of a serious general interest. This criterion shows that the provision is of more than ordinary significance for the society. Pursuant to the principles of proportionality and subsidiarity, this interest must be serious enough for the interest of provision to third parties to outweigh the interest of the protection of the personal privacy of the person to which the police data relate. Thirdly, the decision of the person responsible to provide police data is taken by agreement with the competent authority. In relation to Articles 22 and 23, 'the competent authority' refers to the authority that holds responsibility for the work for which the data were processed.

Article 23
In practice, the police work together in alliances. The need arises here for a structural exchange of data in which the police and third parties have parallel interests. In these alliances, the performance of police tasks is consistent with the interests of the authorities with which the police cooperate. For example, the police force works for the control of youth crime with a wide-ranging group of institutions that are involved with problem youths.
In relation to Article 23, this may also involve cooperation with private individuals, such as retailers in addressing shop crime. Article 23 provides the basis for the provision of data to third parties in such cases. The conditions are laid down in Article 23(1). The person responsible may only decide that police data will be provided to persons or institutions for an alliance to the extent that this is necessary for a serious general interest. This criterion is explained in more detail in the notes to Articles 21 and 22. The provision of police data to third parties as part of an alliance may take place only if the purpose of the provision is consistent or compatible with the tasks of the police. In addition, the requirement of a serious general interest applies. Examples in which a serious general interest may be at issue in the provision of data for an alliance include the control of youth crime, control of domestic violence or the approach to shop crime. Apart from the fact that a serious general interest must be at stake, the purpose of the provision must be consistent or compatible with the police tasks, i.e. the prevention and investigation of crime, the maintenance of public order, the provision of assistance to those in need of this and the performance of supervision of compliance with regulations. With regard to the involvement of the competent authority, the comments made in that regard in relation to Article 22 apply. The decision to provide the police data must state the alliance for which the data are provided as well as the purpose for which this was formed, which data will be provided, the conditions on which the data will be provided and the persons to whom or the institutions to which the data will be provided.

Article 24
This paragraph offers the possibility of laying down further rules by or pursuant to national decree containing general measures, with regard to the categories of police data that are or may be provided pursuant to Articles 21, 22 and 23. If necessary, certain data may be excluded from provision to third parties in this way. This could involve sensitive investigative data, such as certain data from current criminal investigations, data being processed under the regime of Article 13 or data regarding informants who are pursuant to Article 15.

Article 25
In certain cases, there is a need for police data for scientific research and for policy data. To that end, the registers should be opened subject to the necessary assurances. By national decree containing general measures, rules will be laid down regarding this. There are objections to the direct regulation of this subject matter in the national ordinance due to the fairly extensive casuistry. The national ordinance does include, as a general standard, that the results of the scientific research may not contain any data that can be traced to individual persons. The generally sensitive nature of the data recorded in police registers makes it necessary to exclude the use of these for e.g. historical research in which the conduct of individual persons is discussed.

§ 4. Rights of the person concerned

Article 27
The right to viewing is based on the principle, which is also laid down in international treaties, that a person concerning whom personal data are processed by the police must be given an opportunity to view those data, partly with a view to exercising his right to correct or delete such data. This means that in principle, everyone must be given an opportunity to determine whether their data are processed and if necessary, to contest such processing in law. Reference can also be made to Article 13 of the European Convention on Human Rights (ECHR) in that regard, which provides that everyone whose rights or freedoms under that convention have been breached has a right to an actual legal remedy for a national institution. Respect for privacy is laid down in this convention (Article 8 of the ECHR). However, the right to access data is not an absolute right, as it may be restricted if this is necessary in a democratic legal system in interests including combatting crimes. An investigation could be seriously frustrated if suspects of criminal offences became aware of certain police data in the course of a criminal investigation and adapted their behaviour in such a way that, for example, the deployment of special investigative powers became illusory. The draft

therefore offers the manager the possibility of refusing viewing access in connection with the proper performance of police tasks or with serious third-party interests. In principle, the applicant has a right of access, the grounds for rejection assume an assessment in each individual case. In connection with the enforceability of the regulation, a number of adjustments are proposed, which will be discussed below.

Paragraphs 1 and 2 Applications for access must be made in writing. This condition arises from the demands on the capacity of the police, imposed by the sharp increase in the number of applications for access in recent years. Partly in connection with this increase, the police cannot be expected to conduct exhaustive investigations into the processing of police data in cases in which requests for access provide no leads for this. A written application is expected to provide more concrete leads than an oral request. Moreover, an application in written form offers the police the opportunity to account for the manner in which they respond to the application after the event.

Article 28
This Article contains a number of formalities concerning the handling of the application.

Article 29
This Article proposes grounds for the rejection of an application as referred to in Article 27. The criterion of 'proper performance of the police task' covers the prevention, investigation and prosecution of criminal offences but also relates to the maintenance of public order and the provision of assistance. The proper performance of the police task can also be invoked as grounds for rejection of access applications that are apparently only intended to burden the police organisation. Both in the case in which data on the applicant are processed and where this is not the case, it may be necessary in view of the interests referred to in this Article to provide no notice of this. In cases concerning data on informants or infiltrators, for example, due to the risks for the safety of persons it may be necessary to withhold access to the data, or to part thereof, to the extent that access could give rise to risks for the informant or for third parties. In the first instance, this could concern data on the identity of the informant. In some circumstances, this may include other data from which the identity of the informant can be deduced for the person concerned, such as name and address details, data from reports on meetings, data on remuneration and the like.

Article 30
This Article imposes rules concerning the correction, supplementation, removal or hiding of data.

Article 31
Paragraph 1 establishes beyond doubt that a decision by the person responsible concerning an application for access, correction, supplementation, removal or hiding of data is deemed to be an administrative decision within the meaning of the National ordinance administrative justice.

Article 32
An obligation applies for the person responsible to notify all persons to whom or institutions to which police data were provided in the year preceding that of an application for access of the correction, supplementation, removal or hiding of that data. On request, the person responsible informs the applicant and, where applicable, the legal representative of the parties that he has notified.

Article 33
The person responsible may charge costs for notification, as referred to in Article 27(1), which may not exceed an amount fixed by or pursuant to a national decree containing general measures. The method of payment shall also be laid down here. The payment shall be returned at the request of the person concerned or on the order of a court, if the person responsible failed to perform the correction, supplementation, removal or hiding pursuant to Article 29.

§ 5. Supervision

Article 34

The requirement of authorisation applies for the processing of data within the police force. The aim of the authorisation requirement is to ensure that processing takes place only to the extent that this is necessary for the proper performance of the police officer's tasks. The person responsible is responsible for the system of authorisation and for correct implementation of this, to the extent that police data are processed under his management. Pursuant to Article 4, the person responsible must implement appropriate technical and organisational measures to secure police data against unlawful processing, among other things. In addition, supervision and control are exercised on the lawful processing of data on the grounds of Articles 35, 36 and 37. In order to enable both internal and external supervision, the person responsible must record certain instances of processing. This protocol obligation is laid down in Article 34. This Article underscores the fact that the person responsible is responsible for the written recording and ensures that supervision and control are possible, for example on the basis of the written record of the purposes of processing pursuant to Articles 12 and 15. The obligation to record the provision of police data to third parties also serves for the possibility of informing such persons or institutions after the event in the case of the correction of data. The person responsible is also required to record processing regarding which there are indications of unauthorised use. This may be the case if data are processed by persons who are not authorised for such processing. To that end, the person responsible may compare 'user profiles' with behavioural profiles in order to identify any irregular or unlawful processing. The system of audits may also be set up in such a way that, for example through random tests, any unlawful processing can be brought to light.

Paragraph 2
The term for saving written records is closely associated with the purpose of the processing. It stands to reason, for example, to cease written recording of the purpose of an investigation as soon as the purpose of that investigation has been realised and the relevant investigation data have been removed pursuant to Article 12(4). The written record of an authorisation must in any event be kept for as long as the authorisation applies. In order to prevent data from being destroyed before control of the implementation of the rules laid down by or pursuant to this national ordinance has taken place, the term for saving certain data has been linked to the performance of audits, as referred to in Article 35. In order to be able to perform adequate supervision, the data must remain available at least until the audit has been completed.
If a new control is performed, the data must remain available until the new control has been completed. In addition, the record of the provision of data will be needed at a later stage if an access application has not yet been settled when the control is completed. The person responsible must keep the record for as long as is necessary for compliance with that obligation. Thereafter, removal can take place.

Article 35
In order to ensure that the limits proposed by the draft are not exceeded in practice, it is important to create appropriate assurances. The draft provides for this in two forms of internal supervision. Firstly, the draft requires the person responsible to provide for regular evaluations and privacy audits for control of compliance with the national ordinance. The requirements formulated in the national ordinance must be implemented effectively within the police organisation in order to secure the rights of citizens in an adequate manner. It is therefore important to realise an adequate system of general processing measures and procedures, taking account of the specific protective measures that are necessary for the processing of police data. In order to arrive at a balanced policy for the processing of police data and to implement and maintain this adequately, it must hold an important position in the management cycle. Secondly, the national ordinance requires the person responsible to appoint a privacy officer. This officer's tasks include control of the processing of the data and advising the person responsible with regard to compliance with this national ordinance. With the aid of a monitoring system (evaluations and privacy audits), the person responsible must determine the extent to which the processing measures and procedures laid down realise the objective of the legal standards and the privacy policy formulated. The results of the monitoring performed form the basis for any corrective action, adjustment of the measures and procedures laid down, or modification of the policy formulated. In conducting the privacy audit, an independent auditor primarily examines whether the organisation is adequately designed to comply with the legal provisions satisfactorily. The auditor will then assess the existence of the measures and procedures drawn up by the organisation to provide for the assurance of the legal

requirements. Finally, he will devote attention to the assessment of the operation of the relevant measures over a predetermined period. In order to enable this form of supervision, the person responsible is required to provide the information and data necessary for that supervision. The person responsible is required to provide for regular control of the regulations laid down by or pursuant to the national ordinance by means of an independent privacy audit. This refers to the fact that the person responsible issues instructions to an auditor that is not associated with the relevant organisation to conduct the audit. He will be notified of the outcomes of the examination in the form of a report. If, unfortunately, parts of the processing of police data prove not to meet the quality requirements to be set, a new audit must be conducted within one year of the parts for which the result was inadequate. If, following this new audit, the processing of data still fails to comply with the requirements to be set, a further audit must be performed within one year, etc., until such time as another regular audit must be conducted. The costs of any new audit are borne by the person responsible. For the purpose of the audit, employees of the agency that performs the audit must have access to the data systems or data files in which the police data are kept (Article 4(5)). They must protect the confidentiality of the police data of which they become aware (Article 10). The audit cycle and the manner of conducting the audits shall be developed in more detail by national decree containing general measures. Rules will be imposed here for the requirements to be made of the auditor, including rules in relation to the screening and the firms of auditors that are authorised to conduct the reviews and the privacy audits. These firms must comply with specific requirements to be imposed in the field of the organisational and administrative design of the organisation and for the knowledge and experience of the experts required in order to conduct the audits. Within the set frameworks, the person responsible must select a firm of auditors that will be instructed to conduct the review or the privacy audit. Rules will also be imposed with regard to the regular assessment of the set requirements and the payment of the costs to be incurred by the person responsible. The advice of the Law Enforcement Council will be requested on the draft of the national decree containing general measures. A copy of the audit report will be sent to the Law Enforcement Council. If necessary, the Council may also access the reports on the self-evaluations and the reviews, on the basis of its general supervisory powers.

Article 36
In this Article, the person responsible is required to appoint a privacy officer. The task of the privacy officer, as referred to here, is to supervise the processing of data on behalf of the person responsible and to advise the person responsible regarding compliance with this national ordinance. Pursuant to Article 4(4), the privacy officer has access to the police data that he needs for his task. The privacy officer must have a review of the investigations taking place pursuant to Article 12(1). As soon as an Article 12 investigation is opened, this must be reported to the privacy officer, as well, of course, as any changes in the purpose-specifications and closure of investigations. The privacy officer also maintains an overview of the authorisations within the force. The privacy officer can play an important role in supporting the person responsible in the (internal) control and supervision of the processing of personal data, and can also provide data on the organisation and implementation of working processes and on the granting of authorisation and for processing of data. He can also play an important role in the right to access and correct police data.

Article 37
External supervision of compliance with the national ordinance is assigned to the Law Enforcement Council. The Council's authorities pursuant to Articles 22 up to and including 27 and Article 20 of the Law Enforcement Council are declared to be likewise applicable.

§ 6. Final provisions

Article 38
This draft contains a large number of rules and regulations concerning the processing of police data, some of which will be developed in more detail by or pursuant to national decrees, containing general measures. In order to be able to tailor the legislation closely to new developments and to be able to take account of specific implementing aspects, a general evaluation provision is proposed, which provides that the effects of the national ordinance should always be investigated as a whole. A term of five years for this is reasonable.

Article 39

Article 39 provides for the possibility of differentiated entry into force of the national ordinance. This is necessitated by the fact that the implementation of this draft depends partly on the introduction of data management. If necessary, a longer term will be chosen for the entry into force of certain Articles before the national ordinance enters into force.