TRANSLATION OF THE OFFICIAL PUBLICATION OF SINT MAARTEN (AB 2010, GT no. 4)

EXPLANATORY MEMORANDUM

1. General

As a result of the dissolution of the country of the Netherlands Antilles (NA), the services and ministries of the NA will be closed after a dismantlement period. The tasks performed by these institutions are now performed by the government bodies and institutions of the new Countries within the Kingdom. This is also the case with regard to the national security task, which was performed in the Antilles by the Netherlands Antilles Security Service (NASS). This security service, which formed part of the NA Police Force, was formed to implement Article 4(4) of the Police Regulation (PB 1962, No. 64). The tasks and the organisation of the NASS were briefly described in a national decree (PB 1963, No. 89); at the time, attention focused largely on persons and extremist movements that represented a danger to the state.

With the formation of the country of Sint Maarten, provision for national security will be the responsibility of this Country. Government provision for national security, which, as an umbrella term, covers the continuation of the democratic legal order, the integrity of public administration and the security and other important interests of Sint Maarten, will be realised through the formation of a Sint Maarten Security Service, hereinafter referred to as 'the service' or 'SMSS'. The service provides for national security partly by identifying in good time the threats to the interests of the state and risks that are not directly visible, and monitors, advises and mobilises. This makes the SMSS a necessary part of the government organisation and of the network that protects national security.

The service will, for example, supply information (on threats) on the basis of which other parties (such as the police) can take appropriate security measures. This may be the case if, for instance, investments or other use of financial institutions and facilities are made for money flows of terrorist organisations operating internationally, or another form of terrorist threat in Sint Maarten. The police and other interested parties are then responsible for taking the appropriate security measures, as the SMSS is not a detection or prosecution agency.

This ordinance is based on, and corresponds closely with the existing legislation concerning intelligence and security services within the Kingdom, namely the 2002 Dutch Intelligence and Security Services Act (Wiv 2002) and the Aruban National Security Service Ordinance.

By their nature, the activities of intelligence and security services entail a restriction of the citizens' rights of privacy. After all, processing of personal data in general, and the deployment of (special) powers in the gathering of such data in particular, constitute a restriction by these services of the right to privacy laid down in both the Constitution of Sint Maarten and in the European Convention on Human Rights and Fundamental Freedoms (ECHR, Article 8), as well as other fundamental rights. However, both the Constitution and the ECHR permit this, provided that certain requirements are met. Article 8 of the ECHR grants everyone the right to respect for his private and family life, his home and his correspondence. Pursuant to Article 8(2) of the ECHR, there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of (among other things) national security. It follows from this provision, firstly, that a regulation in which powers are assigned to intelligence and security services that entail a restriction of the right guaranteed by Article 8 is included in national law and that this is sufficiently foreseeable and identifiable for the citizens. The powers must be formulated precisely enough and the regulation must provide assurances against random interference with personal privacy. The proposed powers must also be necessary in a democratic society. There must be a 'pressing social need' that justifies the breach and makes the breach proportionate to its purpose. The jurisprudence of the European Court of Human Rights allows the national states a certain 'margin of appreciation' in meeting this requirement. Article 31(1) of the Constitution also provides that a restriction of a traditional constitutional right must be necessary and proportionate, and must be described as specifically as possible.

In the view of the government, this regulation, which, among other things, regulates the institution, tasks and powers of the SMSS, but also provides for an independent supervisory authority (the Supervisory Committee), meets the requirements arising from both the Constitution of Sint Maarten and the ECHR.

In the formation of a security service such as the SMSS, the government devoted special attention to the operation of this organisation within the framework of principles underlying a democratic state under the rule of law, as applying in Sint Maarten. There is inevitably a degree of tension here between these principles and the working methods of such a service. A democratic state under the rule of law cannot generally function well without a high degree of open government and effective political and judicial control. A security service, however, only functions effectively if its activities remain unnoticed as far as possible and are not public. This means that the SMSS, in terms of open government and control, cannot be equated with other government services that operate in the field of general administration. For this reason, it is not only important to record the rules with which the SMSS must comply in the performance of its tasks as clearly as possible, but also to describe the special powers that it needs for its work as precisely as possible. It is also important that clear assurances for citizens are included in this ordinance. In view of the nature of the work of the service, the application of the usual supervision of government services is not possible to the same extent, as a result of which provision has been made for adjusted control instruments regarding the tasks performed by the SMSS. This ordinance is formulated in such a way that the presence (or absence) of provisions concerning a number of general principles clearly shows what the SMSS, and in particular the head of the service, must take into account in the performance of its duties. These principles are:

a. in the performance of its duties, the SMSS is bound by the law (treaties and ordinances) and must work in a proper manner with due care – in this case, this rule, which applies for every government service, is recorded explicitly (Article 2);
b. the SMSS shall continually keep the Prime Minister, Minister of General Affairs, hereinafter referred to as 'the Minister', informed of its activities and of the information obtained in this which is important for him, as only in this way can he bear full ministerial responsibility for the operation of the SMSS and meet his control and supervisory tasks in relation to the service (Article 3(2));
c. there shall be a supervisory mechanism, to which end it is laid down in law that in addition to the supervision of the Minister, additional supervision of the performance of the tasks of the SMSS is performed by the Supervisory Committee (Chapter 11);
d. when gathering data, the SMSS should always have a concrete goal that falls within the statutory duties of the service. This means that gathering of data by the personnel for purposes that fall beyond the tasks set (or without a specific purpose) is not permitted (Article 9);
e. the SMSS does not concern itself with the detection of offences (Article 4(2) and 7(3));
f. for the application of special powers, there is a consideration framework embedded in the ordinance: necessity, subsidiarity and proportionality (Chapter 5, in particular Article 26);
g. the categories of persons who may be the subject of an investigation are described exhaustively; in other words, neither the personnel nor the head are permitted to gather data on other persons (Article 10);
h. inquiries concerning persons may not be specifically directed at a person's religion or belief, race, health or sexual life (Article 10(2));
i. when and how the data gathered by the SMSS is obtained must always be recorded (Article 9(4));
j. the work of the SMSS is never associated with the application or threat of physical or mental violence (as may be the case, for example, with the police). This latter principle leads, among other things, to the absence of powers for SMSS personnel to use violence;
k. in connection with the possibility for the Minister to take disciplinary measures, the personnel (and the head) are civil servants, within the meaning of the National Ordinance substantive civil servants law (PB 164, No. 59) Article 4(1) and Article 7(1)). A special position is assigned to the SMSS itself, within the framework of the accountable system, in connection with the creation of financial control consistent with the duties of the service (Chapter 14).

2. The draft in outline

This concerns a government service, the operations of which, by their nature, inevitably lead to infringements of the constitutional rights of the citizens at certain times. Chapter 2, Constitutional Rights, of the Constitution van Sint Maarten requires that provision for infringements of the constitutional rights of the citizens are always laid down at the level of the national ordinance. This applies, for example, for Article 5 (the right to respect of privacy), Article 7 (laying down the right to respect for the privacy of the home) and Article 8 (confidentiality of correspondence and telephone conversations) of the Constitution of Sint Maarten. The government therefore decided to lay down the tasks of the SMSS in a national ordinance.

2.1. General provisions

The terms frequently occurring in the ordinance are defined in Chapter 1. The term 'data processing' (or processing of data) holds a key position in the performance of the tasks by the service. This concerns processing of data in the broadest sense of the word. The definition concerns the processing of personal data

and other data. 'Personal data' are all data relating to an identifiable or identified individual natural person. The term 'other data' may concern, for example, data concerning a particular organisation, such as the financial data of the organisation, or certain social phenomena.

2.2. Objectives and tasks of the SMSS

Chapter 2 concerns the tasks of the SMSS. The term 'national security' is used as an umbrella criterion for the performance of the tasks of the service. The term 'national security' is drawn from Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). The first paragraph of the aforementioned Article lays down the right to privacy. National security is one of the objective criteria on the grounds of which the government may restrict this right (grounds for restriction, Article 8(2)). In the jurisprudence of the European Court of Human Rights (ECHR), a 'wide margin of appreciation' is allowed for the definition of the term 'national security'. The term 'national security' is not only intended to cover the performance of the tasks by the service, but also to regulate and limit the performance of those tasks. It can be deduced from the jurisprudence of the ECHR concerning Article 8 that national security may, for example, be at issue in the violation of state and military secrets, the call to, and approval of violence, the performance of terrorist activities and the publication of confidential information in documents that could cause harm to the operation of a country's national security service. Partly in view of the interpretation of the term 'national security' in common parlance, this adequately defines the activities of the SMSS. The statutory definitions of the tasks of foreign intelligence and security services also show that these must primarily perform activities in relation to 'national security' or equivalents thereof.

However, the service also performs activities that do not involve infringements of constitutional rights.

The underlying objective of the activities of the SMSS is expressed in Article 3. The fundamental interest of the citizens in the continuation of the existing constitutional system, both in Sint Maarten and throughout the entire Kingdom, normally referred to as the 'democratic legal order', can be classed under the umbrella term of national security, together with other interests such as integrity, security and other serious interests of state. Generally formulated tasks follow from this umbrella objective of 'national security', which, in turn, lead to concrete actual tasks that are aimed at identifying the risks that threaten the democratic rule of law, among other things, and at making proposals for measures to be taken to reduce or control those risks. There must be facts and circumstances that give rise to serious suspicions that there are (or may be) risks to national security before work arises for the SMSS. This entails an important restriction of the authorisation to gather data. The SMSS must always give the Minister sound reason to assume that the gathering of data on persons and organisations is (or was) necessary in connection with the tasks assigned to the service in relation to national security. The SMSS also conducts security investigations into persons who hold key positions for the country or elsewhere in Sint Maarten (for example in the business community) that provide a possibility of harming national security, i.e. positions involving confidentiality. A security investigation is conducted only if the person concerned has given written consent for its institution (Article 3(1)(b)).

Finally, the service is mandated with a task on the level of promoting security. This task is of a preventive nature and includes advising on measures to be taken to protect state secrets (Article 3(1)(c)).

Chapter 2 then covers the minimum requirements that the head of the SMSS and the personnel must meet and the other responsibilities of the head. It also explicitly provides that the head and the personnel have no detection authorisation. The SMSS is therefore not a service charged with executive powers.

The principle of ministerial responsibility applies in full, as a result of which the Minister can impose further rules concerning the organisation, working method and management of the service if he considers this necessary, for example, following talks in the Council of Ministers, on the grounds of an explicit request from Parliament (Article 8).

The head of the SMSS is appointed on the joint nomination of the Minister and the Minister of Justice. The aim of this is to provide a sound basis for the cooperation which will exist in practice between the services operating in the judicial chain, such as detection services and the Department of Public Prosecutions on the one hand, and the SMSS on the other. See also Chapter 10.

It is a fact that a security service cannot function effectively without a high level of confidentiality. The head therefore bears a special responsibility. He must provide for effective protection against disclosure of all information held by the SMSS and of the sources of that information. His responsibility for the security of the persons involved in gathering data is directly related to this (Articles 5 and 6).

2.3. General provisions concerning the processing of data
The SMSS conducts investigations into potential threats to our national security. As part of those investigations, the SMSS processes data: this is the core business of the service. With regard to the data processing, as defined in Article 1 of the ordinance, a number of general provisions are laid down in Chapter 3. These provisions therefore apply to all forms of data processing, such as the gathering of data and the provision of data. Moreover, a number of special additional provisions are laid down in the ordinance with regard to some specific forms of data processing, such as the gathering and provision of data by the services. This is discussed later in this explanatory memorandum.

Chapter 3 (Article 9) provides, among other things, that the processing of data is justified only in observance of the requirements laid down by or pursuant to the ordinance, that data processing may take place for a specific purpose only and then only to the extent necessary for proper performance of the tasks of the service. Processing must also comply with the law and take place in a proper manner with due care. Furthermore, the data must be provided with an indication of the degree of reliability or a reference to the document or the source from which the data are derived. The latter is important in order to determine the value that must be assigned to particular data, which is important in view of the potential repercussions for the person or organisation to which the data relate.

Investigations by the SMSS may concern persons and organisations regarding which it is necessary to gather and record data. The categories of persons who may be the subject of investigations are described exhaustively in Article 10, and personnel are not permitted to gather (or save) data on other persons. This Article therefore prevents random maintenance of files on everyone who resides in Sint Maarten. Moreover, investigations concerning persons may not be specifically directed at a person's religion or belief, race, health or sexual life.

Finally, Article 11 provides that incorrect data must be improved and that personal data that are no longer necessary must be deleted and destroyed in accordance with rules laid down by national decree.

2.4. General powers to gather data
The general powers referred to in Chapter 4 include the gathering of data from public sources and obtaining information from persons and institutions. Obviously, no further rules or conditions need be set with regard to the former activity: what every citizen has a right to is also permitted for government services. This includes for instance consulting newspapers, television and the internet. The situation is somewhat different when information is obtained from individual citizens and institutions. The main rule here is that those who are contacted are free to provide or not to provide the required information; in general terms, there is no obligation to provide assistance for the activities of the service, including the provision of information. Article 14(3) makes an exception to this principle. A person responsible for the management of a government service must provide the head of the SMSS with the required information on request. To the extent that this concerns information that is subject to a special confidentiality obligation, provision is made for a special procedure that should contribute towards a good consideration of interests. If the relevant information is then provided, the special rules applying to such provision do not apply in that case.

It also follows from the text of Article 14 that a party responsible for data processing (such as a bank) is not required to provide data to the SMSS. However, if the responsible party does decide to provide data to the SMSS, this Article provides that the rules applying for the responsible party with regard to the provision of such data do not apply (indemnification provision). Thus, for example, the processing of certain (personal) data is often justified only for a particular purpose, where often, as a secondary purpose, no provision is made for any supply of data to the SMSS. In cases of that kind, in accordance with Article 14(4), the legal provision concerning objective-bound processing is derogated, so that the provision to the SMSS can take place legitimately.

2.5. Special powers to gather data
In addition to the general powers to gather data, for which Chapter 4 lays down rules, the ordinance also provides for the possibility for the service to apply 'special powers' in data gathering. These powers are generally deployed secretly and are often more far-reaching in nature with regard to the privacy of citizens. Partly in view of this, the deployment of these special powers is permitted only in the case of inquiries by the service in relation to the task imposed in Article 3(1)(a), i.e. in inquiries into (unidentified) threats to the national security of Sint Maarten (Article 15). These special powers may not, therefore, be deployed in security investigations.

The special powers are listed exhaustively in Article 17. This concerns the following special powers:

a. the observation of natural persons or goods and the recording of data in that regard, with or without the aid of observation and recording tools;
b. following of natural persons or goods and the recording of data in that regard, with or without the aid of tracking devices, locating equipment and recording tools;
c. entry to and searching of enclosed locations;
d. opening and inspection of closed objects;
e. tapping, recording and monitoring of conversations, telecommunications or automated data transfers by technical means;
f. the incorporation and deployment of legal entities to prepare and support operational activities;
g. the deployment of natural persons, not being personnel, who are mandated, with or without the use of an assumed identity or capacity, occasionally or for a specific term, under the responsibility and on the instruction of the service, to:
    1° gather specific data concerning organisations or persons which may be of importance for the performance of the service's tasks,
    2° the promotion or taking of measures and the performance of actions as referred to in Article 23(3) to protect the interests to be represented by the service.

Efforts have been made in this ordinance to formulate the special powers as free of technology as possible, in view of the rapid rate of technological development, and with as little risk of outdating as possible.

However, as it cannot be ruled out entirely that, for example, as a result of technological or other developments, possibilities become available to gather data that cannot be based on one of the powers provided for in Article 17(1), Article 25 provides for a regulation on the basis of which, under special conditions, the relevant action can nevertheless be performed (or the relevant tools can be deployed). In that case, the government must submit a draft national ordinance regulating this to Parliament within six months of granting consent for this. If this does not take place, continued application of this is no longer justified.

Further rules, both general and tailored to the relevant special powers, are laid down in Article 17 and in the subsequent Articles. Among other things, this involves rules that provide for the granting of consent (by the competent institution), the procedure to be followed for obtaining consent and the assessment framework to be used.

In general, the prior written consent of the Minister is required for the use of one of the special powers described in Chapter 5, or of the head on behalf of the (mandate of the) Minister (Article 16(1)). The head can delegate this power to a subordinate member of his personnel, but must immediately report this to the Minister. The deployment of weightier methods such as opening letters, tapping telephone calls and entry to residential properties without the consent of the occupant requires the prior written consent of the Minister in each case (Article 17(3)). Such consent applies for three months only and can be extended at the written request of the service. In addition, the authorisation of a judge employed at the Court of First Instance, sitting in Sint Maarten, is required for opening letters without the consent of the addressee.

Articles 18 up to and including 22 lay down specific rules with regard to a number of special powers. Where necessary, this is discussed in more detail in the Article by Article section of this explanatory memorandum. The assessment framework to be observed in the application of these special powers is considered here. In addition to the general necessity requirement in Article 15, this assessment framework is developed further in Article 26 and, in line with the requirement for this laid down in the ECHR, aims to provide for an extensive system of assurances that ensure that conflicting interests are assessed with care in each concrete case. Application of special powers must meet the requirements of proportionality (how does the method relate to the seriousness of the situation) and subsidiarity (can a less weighty method be applied). Furthermore, this ordinance provides that a written report of the deployment of special powers must be drawn up in each concrete case. This report serves for the performance of the supervisory tasks of the Minister and the Supervisory Committee.

This ordinance includes a further development of the notification obligation with regard to the exercise of the special power to enter a residential property without the consent of the occupant. Pursuant to Article 7(3) of the Constitution of Sint Maarten, there is an obligation to provide the occupant with a written report of the entry within 48 hours in the event of entry of a residential property without the occupant's consent. It is clear that if it proved necessary for the service to secretly enter a residential property as part of the proper

performance of its tasks (for example, in order to install a microphone in the property), for the time being there can be no question of issuing a report; after all, that would seriously harm effective performance of the tasks of the service. In the interests of national security, therefore, the Constitution offers the possibility of laying down rules in that regard by national ordinance to defer the issue of the report and, in cases to be laid down by national ordinance, even to omit this if this is permanently counter to the interest of national security. Article 24 of the ordinance further develops the notification obligation, as well as the cases in which there is a reason to postpone the obligation, or in which the obligation lapses. Before determining whether notification (the issue of the report) is possible, it is necessary to investigate first whether this is possible and whether there are any grounds (for postponement or omission) to prevent this. This investigation obligation does not arise until five years after the termination of the special power referred to here and is reinstated each year in the event of grounds for postponement. The assessment of whether there are grounds for postponement is conducted in accordance with the criteria set in relation to a request to view personal data. It should be clear that if a request to view personal data must be rejected, it is not logical to issue notification, particularly since such notification could precisely lead to a request for access (or a complaint). Finally, it is noted that the regulation also provides that the obligation to issue a report lapses if it is established that this is not reasonably possible. The situation in which the person concerned can no longer be localised (for example because that person has left for an unknown destination) must be borne in mind here.

2.6. Internal and external provision of data

Chapter 6 lays down rules concerning the provision of data processed by the SMSS. A distinction is made here between the provision of data within the service and the provision of data to third parties. The provision of data within the service is permitted only to the extent necessary for proper performance of the task assigned to the relevant civil servant; this concerns the expression of the 'need to know' principle (Article 27). Articles 28 *et seq.* provide for a regulation concerning the provision of data to third parties. It should be noted that the ordinance provides for a closed provision system; only in the cases for which the ordinance provides may the SMSS report processed data. This includes the regulation included in Chapter 7, concerning access to personal and other data (since this is also a form of provision).

The following is noted with regard to provision to third parties is concerned ('external provision'). The SMSS gathers and processes data in relation to the tasks assigned to the service by this ordinance, for which, as already explained, various powers can be deployed. On the basis of Article 3(1)(a), the task has been assigned to the SMSS to conduct investigations into, in short, (unidentified) threats to the national security of Sint Maarten (Article 3(1)(a)). It is clear that if these investigations lead to findings such as information on the threat of an attack, or that a certain person wishing to establish himself on the island presents a national security risk, on the basis of which other institutions can take measures that, for example, could eliminate or reduce the identified threat to the national security of Sint Maarten, data must be (able to be) provided (and notices may also be issued). Alongside the task referred to here, the SMSS is also responsible for conducting security investigations. Data are processed in that regard too; those investigations may lead to the conclusion that a certain person must be refused a certificate of no objection, or that such a certificate must be withdrawn. It must also be possible to issue notices on this, not only to the person concerned but also to their (prospective) employer. Finally, the security promotion task regulated in Article 3(1)(c); in that regard too, it must be possible to provide information processed by the service that could, for example, assist in the taking of security measures. In all the cases mentioned, this concerns the provision of data in relation to the proper performance of the tasks of the SMSS. Article 28 provides for a regulation for this form of provision.

In connection with the Minister's responsibility for the SMSS, with the recognition that the data processed by the SMSS may concern (highly) sensitive information, it is considered desirable with regard to the provision of data externally as part of the proper performance of tasks to provide for a system in which the head of the service is granted general or special written permission to provide data. In the view of the government, this provides substantial assurance that the SMSS (and the civil servants who work there) cannot circulate the data gathered without authorisation. The cases in which the head is authorised, in general terms, to provide data as part of the performance of the tasks will be described in a general written authorisation; a general authorisation is expected to cover the majority of the possible issues of data, including from the point of view of efficient performance of the tasks. For each case that is not covered by the general authorisation, special written authorisation must be requested. In particular, these will be the cases which call for an independent assessment by the Minister, in view of the nature of the information and any political and administrative aspects. Naturally, this does not alter the fact that in the cases in which provision is covered by the general authorisation, too, the nature of the notice (or of the data to be provided) may mean that the Minister is information and issues the notice himself; Article 28(2) provides for this.

The institutions to which data can be provided as part of the performance of tasks by the SMSS are described in more detail in Article 28(1). Pursuant to paragraph 5, every issue of data takes place under two conditions: (1) that the data may be used only for the purpose for which they are issued and (2) that they may be passed on to other parties only with the written consent of the head of the service (in which further conditions may be imposed). The latter condition expresses the 'third party principle'. Apart from the obligation laid down here to invoke this rule as a standard, this rule is a standard condition that is always imposed in exchanges of information between intelligence and security services.

In the interests of supervision by the Minister, the head reports every four months by means of a written report concerning the notices issued on the grounds of the general and special consent granted. A new Minister receives a written review of the general and special authorisations still applicable at that time within 30 days of taking office. That gives him an opportunity to see whether he wishes to pursue a different policy in that regard; the authorisations granted previously remain in effect until such time as they are altered or withdrawn.

In addition to the provision of (personal and other) data as part of the proper performance of tasks, Article 30 of the ordinance provides for the (restricted) possibility (not the obligation) to also provide data in other cases. This firstly concerns the provision of data that may be of importance for the detection and prosecution of criminal offences; Article 30(1), 30(2) and 30(3) develop this in a different way. Moreover, due to the assurances laid down in it (in particular the right of the member of the Department of Public Prosecutions designated for that purpose to view the underlying data for a notice in order to assess the accuracy of that notice), this regulation also applies if the performance of the tasks of the service calls for such a notice. Other cases in which it must be possible to be able to issue notice of data processed by the service are regulated in Article 30(4). If there is evidence of an urgent and serious reason, data may, under certain conditions, be provided to persons and institutions designated by or pursuant to national decree that are involved in the performance of a public task, if that data may be of importance for the protection of the interests for which they are responsible.

Article 32 provides for a further specific regulation for the provision of personal data, the accuracy of which cannot reasonably be established or which were processed more than 10 years earlier and no new data have been processed with regard to the person concerned. The principle is that those data should not be provided. In paragraph 2, an exception to this is made for a limited number of cases in which, pursuant to paragraph 3, accompanying information must be provided in order to place the personal data in the appropriate context.

It is of the greatest importance for citizens that incorrect or incorrectly processed data are corrected or deleted; Article 11(1) lays down rules for this. Provision is also made here for the Minister to issue notice of the improvement or deletion to any recipients of these data.

Finally, a (written) note of the provision of personal data must always be kept. both for internal control and for accounting in connection with supervision (after the event).

2.7. Right to access to personal data and other data

Chapter 7 lays down the main rule that a person concerning whom personal data are recorded may access these, on an application to the Minister, unless this application cannot be honoured on the basis of the grounds for rejection included in this ordinance. Furthermore, every citizen may submit an application to the Minister to access data other than personal data. The procedural rules concerning the application to be submitted, its processing and the grounds on which a request for access may be rejected are laid down in the ordinance.

In principle, applications to access the applicant's own personal data or the personal data of a deceased family member (such as a spouse, child or parent) will be granted, unless they must be rejected on the basis of the grounds for rejection laid down in this ordinance. The SMSS can only perform its statutory duties effectively with a certain degree of confidentiality. Three criteria play a role here: the service must protect the confidentiality of 1. its sources, 2. its *modus operandi* and 3. its current level of knowledge. The request for access can only be granted if the request is explicitly confined to access to non-current personal data on the applicant registered in relation to an investigation concerning which the relevant knowledge is no longer relevant for the proper performance of the tasks of the service. In Article 39, the 'current level of knowledge' ground for rejection, with regard to access to personal data, is developed in more detail. An application to access an applicant's own personal data or those of a deceased close family member or (registered) life

partner shall in any event be rejected if data concerning the applicant or the deceased have been process as part of any investigation, unless:

a. 1° the relevant data were processed more than five years earlier,
   2° no new data concerning the applicant have been processed since then in connection with the investigation as part of which the (older) data were processed (if there is a closed investigation and, for example, there has been a correction of incorrect data present, this is not included in the 'processing of new data'), and
   3° the data in question are not relevant for any current investigation;
b. no data have been processed with regard to the applicant.

If, following an assessment in terms of these grounds, access to the relevant personal data proves not to be impermissible on the grounds referred to in this Article, an assessment must then be made in terms of the grounds for rejection as formulated in Article 40. Article 40(1) contains the 'absolute' grounds for rejection, under which data must absolutely be refused; the relative grounds for rejection are laid down in the second paragraph, in which case, consideration of the interests must take place. Thus personal data that provide a view of the sources or *modus operandi* of the service must always be refused on the ground that access to these would harm national security (absolute ground for rejection). The foregoing also applies *mutatis mutandis* for access to personal data of the deceased family members referred to above.

If the assessment in terms of the criteria of Article 39 leads to establishment of the fact that current personal data are involved, the application for access to these must be rejected. It should be clear that in such a case, the fact that there are current data concerning the person concerned cannot be notified, as this provides a view of the current level of knowledge of the service (in particular that the person concerned has attracted the attention of the service, or has done so in the past five years). Conversely, if no personal data at all are recorded, notice of this also provides a view of the current level of knowledge of the service. After all, through such a notice, applicants who know that they could be known to the SMSS due to their actions will discover that their actions have remained hidden to the SMSS. In both cases, it must therefore remain undisclosed whether there are current data or no data. In connection with the general justification requirement for the rejection of an application for access to personal data and the observation that this cannot be honoured in the case in question, this has led to the provision in Article 39(2) that reference to all the grounds for rejection referred to in paragraph 1 should be made only in general terms.

In addition to a regulation for access to personal data, the ordinance provides, in Article 36, for the possibility of submitting an application for access to data other than personal data in relation to an administrative matter. The grounds for rejection described in Article 40 apply (solely) for the assessment of such applications. Article 39, which develops the 'current level of knowledge' criterion in more detail in relation to personal data, does not, therefore, apply. In the cases at issue here, the assessment in terms of the current level of knowledge lies in the assessment in terms of the absolute ground for rejection that provision of the data may harm national security.

As with requests to access personal data, when other data are concerned, the data found must also be assessed in the light of the grounds for rejection and, to the extent necessary, must be screened. Longer terms apply for the processing of these applications (three months, with the possibility of extending this by four weeks on one occasion only) for that reason, and moreover, there is a heavier administrative burden in connection with the handling and screening of these applications.

The possible means of access to the data are developed in more detail in Article 38. Various modalities are available here, and the Minister must take account of the preference of the person concerned and the interests of the service.

A person who has accessed the data concerning him may, if he sees grounds to do so, issue a written declaration that will be added to the data. This may be the case if, for example, the person concerned takes the view that the relevant data are inaccurate or wishes to make his views on these known in other respects. However, this right is not a right of correction.

Finally, it is noted that a special regulation is included in Article 42 for persons who are or have been employed by the service, where this involves access to the data on the person concerned that is recorded in the personnel and salaries administration. After all, this involves an employer-employee relationship. The aforementioned grounds for rejection do not apply, albeit that data that can provide a view of sources should also be kept confidential in this case. Furthermore, (former) members of the staff have a right of correction.

2.8. Security investigations
Conducting security investigations is one of the tasks of the SMSS (Article 3(1)(b)). Chapter 8 lays down the rules that are applicable for this. A security investigation is an investigation aimed at determining whether there are any objections from the point of view of national security to the filling of the relevant position involving confidentiality by the (candidate) confidence official in question.

Pursuant to Article 43, positions involving confidentiality are designated by national decree, containing general measures. Positions involving confidentiality may be positions in government, in the private sector or at other institutions. These positions have a common feature, namely that they offer the possibility of causing harm to national security. The rules laid down in this chapter make it clear (prohibitive provision) that positions involving confidentiality may be held only by persons who have proved, through a security investigation, not to represent a risk to national security (covering the democratic legal order, the integrity of public administration and the security and other vital (economic) interests of the Country). It is also important that a security investigation can only be instituted with the prior written consent of the person concerned. Naturally, the consequence of a refusal to grant consent to an investigation is that no appointment to the relevant position will follow. Security investigations are repeated regularly, every five years (obviously, providing that the person concerned still holds the relevant position) or on the grounds of exceptional circumstances. The consent of the person concerned is not required for a new security investigation (after five years or on the grounds of observed facts or circumstances that give rise to this) (Article 45(1)). The Minister will withdraw a certificate of no objection that has been issued if it must be assumed, on the grounds of the investigation, that it is no longer justified to retain the relevant person in a position involving confidentiality.

Furthermore, the government considers it self-evident that the competent authority or the employer is required to order the person concerned to cease his work immediately following the withdrawal of a certificate of no-objection, or its non-issue in the case of the appointment of the person concerned in anticipation of the completion of the security investigation and should then remove him from the position that he holds at the earliest opportunity. This need not mean automatic dismissal for the person concerned, but could also lead to a transfer, i.e. appointment to a position that does not involve confidentiality. Any notice of objection filed on the grounds of the failure to issue a certificate of no objection, or against the withdrawal thereof, shall be handled by the Supervisory Committee. For the record, it is noted that the security investigation and the refusal or withdrawal of a certificate of no objection is separate from the potential consequences that the refusal or withdrawal of the certificate may have, in effect, for the legal position of the person concerned. Those consequences and the right to litigate against these, or the institution of legal proceedings against these, is governed by the law on civil servants or labour law and cannot form part of action against the order to refuse or to withdraw the certificate as such.

Finally, it should be noted that pursuant to Article 44(3), rules may also be imposed by national decree, containing general measures with regard to the way in which security investigations are conducted (among other things).

2.9 Cooperation between services
Chapter 9 discusses the cooperation between the SMSS and other intelligence and security services. Within the Kingdom, the SMSS will work closely with the Security Service of Curacao (VDC), the Security Service of Aruba (VDA), the General Intelligence and Security Service (AIVD) and the Military Intelligence and Security Service (MIVD). There is already a long history of cooperation between the (former) NASS, the VDA and the AIVD. Cooperation between the intelligence and security services of the Countries of the Kingdom takes place on an entirely voluntary basis. The subject of 'national security' is not included in the full list of matters for the Kingdom in the Charter for the Kingdom of the Netherlands (Charter, Articles 3 and 43(2)). Consequently, this subject can be deemed to be a matter that the individual Countries of the Kingdom represent themselves independently, pursuant to Article 41(1) of the Charter. A covenant between the new partners (Countries) within the Kingdom which includes the willingness in principle to cooperate, will provide a framework for the cooperation, including in the field of security investigations (= investigations for positions involving confidentiality). The cooperation will include the organisation of expert meetings and regular contacts between the heads of the services. The countries may also decide on ad hoc alliances with a view to implementing specific investigations and, where necessary, the services can provide each other with technical and other forms of support.

In addition to contacts with intelligence and security services within the Kingdom, the SMSS will also build up and maintain contacts with qualifying intelligence and security services outside the Kingdom. Article 47

provides the framework for this. In contracting alliances, as well as in determining the nature and degree of cooperation, assessments will always need to be made, partly in the light of aspects of the democratic embedding of the relevant service and the handling of human rights and the like. In relation to the 'maintenance of connections' (cooperation) with other intelligence and security services, data may be provided to these institutions (see Article 47(2) and 47(3)). This possibility of provision exists alongside that of Article 28, which regulates provision in relation to the proper performance of the SMSS's (own) tasks. Article 47 provides for the possibility of also providing data in other cases, under certain conditions, for interests to be represented by these institutions, to the extent that (1) these interests are not inconsistent with the interests that the service represents and (2) provision is not counter to the proper performance of the tasks of the service. This therefore requires assessment on a case-by-case basis. The same assessment framework is also applicable applies if these institutions are provided with technical and other forms of support (on request). The written request to this effect, with an accurate description of the form of assistance required, must be signed by the competent authority of the other service and requires the consent of the Minister.

The field of work of the SMSS lies in the interior and in general will make use of its domestic network for foreign intelligence and, to the extent that this is available, of the information obtained from the partnership with other intelligence and security services (within and beyond the Kingdom). The service will also focus independently on gathering intelligence on and in other countries in cases arising, if there is an external threat to the national security of Sint Maarten, this may even be necessary.

2.10. Cooperation with other institutions

In order to structure the cooperation between the SMSS and other institutions, rules are laid down for this in Chapter 10. Particularly where institutions or organisations whose work has links with that of the SMSS are involved, it is necessary to avoid duplication or even working at cross purposes. In order to avoid this, structured forms of consultation, cooperation and exchanges of information have been created in many democratic countries; this ordinance also provides for this. The problem of restricted lines of communication with other sectors of the government arises with all government services, but failure to provide for such structures can have extremely undesirable repercussions in relation to highly sensitive material such as that with which the SMSS works. Because of the great importance of preventing such consequences, a number of consultative and cooperative relationships are therefore required by law.

Firstly, this concerns the cooperation between the SMSS and the Department of Public Prosecutions. Both institutions have their own tasks, powers and working methods, which are laid down in law. These must also remain separate, but nevertheless, it is highly desirable for the optimal performance of both institutions that the head and the Solicitor-General serving in Sint Maarten, and, if necessary, the Attorney-General, conduct regular talks with each other. The ordinance also contains an obligation for regular talks, jointly or otherwise, between the Commissioner of Police, the chief public prosecutor, the inspector of customs and excise (as the person responsible for customs inspections) and the director of the service responsible for the implementation of the National ordinance admission and deportation. Obviously, these talks are subject to the provisions in Chapter 13 concerning the confidentiality obligation.

If police, customs or immigration officers acquire access to data which they should sense could be of importance for the SMSS, they must pass on these data to the head pursuant to the provisions of this Chapter, via the persons responsible for the management of their services (Article 49(3)). Through the formulation chosen, the performance of this task is covered by Article 47(1) (compliance with obligations as a good civil servant) of the National ordinance substantive civil servants' law, non-compliance with which is subject to the sanction of the application of disciplinary measures for the civil servant concerned. Moreover, Article 49(4) opens the possibility that the provision of data, as referred to here may also take place in a direct automated manner (e.g. via an online connection with these institutions). However, if provision is made for this, the technical and organisational measures still to be prescribed (partly in connection with security) must be taken.

Finally, Article 50 contains a regulation on the possibility of providing technical support, both by the service to the institutions responsible for detection of criminal offences and vice versa. A number of procedural provisions are laid down in that regard, particularly in order to secure responsibility for the actual performance of the work.

2.11. Supervision of the service

As for every other part of the machinery of government, the principle of parliamentary responsibility also applies for an intelligence and security service. In this case, Chapter 11 of this ordinance provides for an

accountability obligation for the activities for the SMSS for the Prime Minister, Minister of General Affairs. However, the nature of the SMSS's work means that normally, no detailed public accounting can be made. In a democratic society such as ours, however, it is necessary to also be able to subject an intelligence and security service and the minister responsible for this organisation to effective control. With this in mind, this ordinance proposes that, in addition to the general parliamentary supervision and the budget supervision, an additional control mechanism be created in the form of a Supervisory Committee. This Committee is specifically responsible for the performance of control of the way in which the SMSS performs its tasks (and exercises its powers).

Clearly, in order to perform such an important and serious task properly, this control mechanism (the Committee) must be authoritative and be able to operate entirely independently of the government. For this reason, a Supervisory Committee has been created that consists of the President of the Common Court of Justice of Aruba, Curaçao, Sint Maarten, Bonaire, Saba and Sint Eustatius, a designated member of that court and two '*qualitate qua'* members (membership linked to position), i.e. the vice chairman of the Council of Advice and the President of Parliament of Sint Maarten. In the opinion of the government, the composition of the Committee ensures that the independent view of the Committee carries the necessary weight. In connection with this, provisions are included in this Chapter to secure the integrity and impeccable conduct of the members of the Committee. Under the circumstances described in the relevant provisions, the Minister and the Minister of Justice, acting jointly, may dismiss or suspend a member of the Committee. The Committee shall have administrative support for its work (Article 55).

The ordinance assigns a number of tasks to the Committee:
a. supervision of the legitimacy of the implementation of the provisions of or pursuant to the ordinance;
b. the provision of information and advice to the Minister concerning the findings of the Committee, on request or otherwise;
c. the investigation and assessment of complaints concerning the actions of the service.

Supervision of the lawful implementation of the ordinance involves supervision after the event. This supervision does not include supervision of effectiveness aspects associated with the performance of the tasks; that form of supervision lies (partially) in the hands of the General Audit Chamber. The independence of the Supervisory Committee, hereinafter referred to as 'the Committee', is reflected partly in the fact that the Committee itself decides whether and if so, which investigations it wishes to open. It does not, therefore perform its work on assignment. It may, of course, be the case that the Minister requests an investigation of the Committee; this right is even laid down in the ordinance for a majority of the Members of Parliament (Article 56(2)). Pursuant to this ordinance, the Committee is authorised to receive all required information concerning the implementation of this ordinance of everyone involved in the implementation of this ordinance, and to obtain access to the data gathered by that organisation. No government civil servant in any government service of Sint Maarten therefore has a confidentiality obligation to the Committee in relation to the Committee's tasks.

The Committee shall issue a report to the Minister on every legitimacy investigation, in which it presents its findings and makes any recommendations it may have. A number of rules for the realisation of this report are laid down in Article 56, on the basis of which the Minister has the right to respond to the findings in the (draft) supervisory report before the Committee adopts the report. This offers the Minister the opportunity to check the facts and to ensure that no state secrets are disclosed in the public section of the report. Such information may be included in a confidential section of the report. After the report has been laid down by the Committee and presented to the Minister, the Minister must present his response to Parliament within six weeks. The confidential section of the report and his response to this (also classified as confidential) may, however, be notified to the party chairmen of all the elected parliamentary parties in confidence. The party chairmen of the parliamentary parties have a statutory confidentiality obligation in that regard; they many not, therefore, disclose any of the knowledge they have acquired in that way to anyone, including, for instance, the members of their parliamentary party. In this way, therefore, full parliamentary control of the work of the SMSS can take place.

Another important task assigned to the Committee concerns the investigation and assessment of complaints concerning the actions of the service. Article 58(1) provides that anyone who takes the view that the service has behaved improperly towards him may submit a complaint in that regard to the Committee. This concerns a view of propriety or impropriety that is broader than legitimacy or illegitimacy alone; it may, for instance, also concern the way in which citizens have been treated by the service. The broad powers of the Committee (see Articles 59 and 60) ensure effective handling of serious complaints. Moreover, Article 64(3) of the

ordinance is likewise applicable to the decision that the Committee issues with regard to the complaint. This means that such a (public) decision may not provide any insight into the means deployed by the service in concrete cases (*modus operandi*), confidential sources used by the service or the current level of knowledge of the service. A statutory confidentiality obligation exists in that regard (see, *inter alia*, Chapter 13). However, the Committee does not act as a judicial body, but only investigates the complaint, makes its decision on this and advises the Minister with regard to the question of which consequences its decision should have. The complainant is notified of the Committee's decision, but he final decision on the complaint remains in the hands of the Minister.

Article 57 also assigns another special task to the Committee, that of assessing a ministerial assignment at the request of the head, if the head takes the view that this assignment is counter to the tasks of the SMSS. However, it is not anticipated that a great deal of use will be made of this possibility.

For the record, we note that the formulation of the relevant Articles of this Chapter does not mean that the recommendations of the Committee need to be unanimous in order to be issued, nor that the Committee must always take a unanimous view regarding whether to exercise the powers assigned to it. The absence of statutory provisions in that regard makes this a matter on which the Committee decides for itself, on the basis of rules of order that it shall establish itself (Article 62).

Finally, each year the Committee shall publish a public report on its work, which will be made generally available (Article 61).

2.12. Reporting concerning performance of tasks by the service

The Minister will account regularly to Parliament for the work of the SMSS by means of a written report (Article 64). This takes place both in public and behind closed doors. In addition to the public section, the report may contain a confidential section.

The circumstances under which the resources of the SMSS can be deployed are clarified still further in the obligation to publish a public written annual report, as laid down in Chapter 12, stating the statutory exceptions to that public disclosure. From the point of view of transparency and the application of the statutory control mechanisms, the performance of the tasks of the service should be known as far as possible. Furthermore, it must be clear and foreseeable for citizens when and through which activities they could attract the attention of the SMSS. In that regard, the statutory obligation of the service to draw up a public annual report each year on the preceding year is extremely important. The requirement is set for the contents of the annual report that these shall specifically state the priority areas on which the service focused in the preceding year, as well as the priority areas or tasks on which the service will in any event focus in the current period (the year in which the report is published).

As the Minister sends the public written report on the SMSS, which falls under his responsibility, to Parliament, there is a guarantee that there is control over the SMSS's activities by the people's representation and at the same time, the citizens are aware of the existence of such a public annual report.

The interest of the state includes the (sub) interest of national security. Information that jeopardises national security must be kept confidential at all times. In particular, this concerns data that provide an insight into a. the resources deployed by the service in concrete cases (*modus operandi*), b. confidential sources used by the service, and c. the current knowledge level of the service. After all, disclosure of the said data will mean, among other things, that an insight is provided into the technical possibilities and lack of possibilities in the exercise of special powers by a service or into the knowledge level present at the SMSS. This concerns information of an operational nature that, if it becomes known to persons or institutions that have or require the attention of the service, will enable them to develop counter-strategies, as a result of which the relevant resources can no longer be effectively deployed. Information on the confidential sources deployed by the SMSS, in particular human sources (such as agents and informants) must be kept confidential because otherwise their personal security may be put at risk. Disclosure of information that provides an insight into the current knowledge level of the service must be prevented because knowledge of this can be used to keep threats of attacks on national security secret from a service such as the SMSS. Persons and organisations that (wish to) develop activities that (could) harm the interests that the SMS was created to protect could, if they were aware of the current level of knowledge of the service, adjust their behaviour to this by concealing their work, including from the service. This would make it impossible for the service to operate effectively and to perform its statutory duties.

The annual report presented by the Minister to Parliament is public, which means, however, that restrictions must necessarily be imposed on its contents (see the above statements in that regard). Chapter 12 makes provision for this: the data that, in view of the interest of the state, cannot be disclosed shall not be included in the public report. These and other data that cannot be disclosed, such as the confidential section of the annual report, may, however, be notified to all party chairmen of the elected parliamentary political parties in confidence (excluding the chairmen of parties that have been formed in the meantime through a split from an elected political party). It is conceivable that Parliament will form a special committee for the activities of the SMSS from among its members, in which the aforementioned chairmen of the parliamentary political parties will participate. However, it is up to Parliament to issue an order on this. In this way, parliamentary control regarding these confidential data is also assured.

2.13 Confidentiality
Chapter 13 regulates the confidentiality obligation that applies for everyone involved in the implementation of this ordinance. The confidentiality obligation also applies after the said involvement has ended. In the view of the government, it speaks for itself that assurance of the confidentiality obligation imposed pursuant to Article 285 of the Criminal Code on everyone with regard to national security data, such as that which emerges in the work of the SMSS, has a heavier emphasis there than in government services in general. Moreover, in addition to the above Article, civil servants are also subject to the special confidentiality obligation laid down in Article 62 of the National ordinance concerning substantive civil servants' law. Everyone involved in the work of the SMSS in any way is subject to the obligation to protect the confidentiality of the data to which they gain access in relation to that work and of which they should be aware that these must remain confidential. If, therefore, a civil servant who is (or was) involved in the implementation of the ordinance is called to act as a witness or expert in legal proceedings, he must observe his confidentiality obligation unless the Minister has explicitly relieved him of this.

2.14. Accountability provisions
Chapter 14 lays down a number of special accountability rules concerning the SMSS. It is important that the powers assigned to the General Audit Chamber with regard to the SMSS may only be exercised by the chairman and the secretary. They may be supported in this by the civil servant responsible for the management of the accountants' service of Sint Maarten. Provision is also made that the generally binding regulations for the implementation of the National accountability ordinance only apply to the service if the implementing rules explicitly state this.

2.15 Transitional and final provisions
It is desirable to include a provision in Chapter 15 that enables action to be taken against entities that, in order to fill a vacancy that is designated as a position involving confidentiality, appoint or maintain the appointment of a person at that company or organisation concerning whom no security investigation has been conducted. The foregoing also relates to the situation in which the relevant person has not obtained a certificate of no objection, or whose certificate of no objection has been withdrawn. A similar provision is included in order to enable action to be taken against a company or organisation for failure to provide the assistance required by law in the exercise of special powers by the SMSS; this concerns the cooperation obligation in the reversal of the encryption of data (Article 21(6)) and the installation of technical facilities by the holder of a concession, as referred to in Article 2 of the National telecommunication ordinance in order to tap and record telecommunications (Article 22(2)).

The government does not rule out the possibility that, partly in response to practical experience in the implementation of this ordinance, it will find that it is desirable to impose further rules concerning the implementation of the ordinance. If other legal grounds do not already exist for this, the power for further regulation laid down in Article 73 may be used for that purpose.

Financial implications
To come

Article by Article section

Article 3(1), opening sentence
The term 'national security' is drawn from Article 8(2) of the ECHR, where it forms one of the objective criteria on the basis of which restrictions of the right to privacy guaranteed in Article 8 ('private and family life, home and correspondence') are permitted. Infringements of constitutional rights, such as those that take place in the exercise of the special powers of the SMSS, are permitted only if 'national security' is at stake. National

security may be at stake in the following cases: the disclosure of state secrets and military secrets, the incitement to and approval of violence, the performance of terrorist activities and the publication of (confidential information in) documents that can harm the operations of the state security service of a country. Even without directly creating a relationship with Article 8 of the ECHR, in view of common parlance, the term 'national security' is a good general description of the context within which the activities of the SMSS are performed.

Article 10(1)(a)
Paragraph 1(a) precisely defines the categories of persons regarding whom the SMSS is authorised to gather personal data. The list included in this paragraph is of an exhaustive character, while the descriptions in sub-paragraphs a and b correspond with the tasks of the service laid down in Article 3(1)(a) and 3(1)(b).

Article 12
The National ordinance security service provides for an exhaustive regulation for the processing of personal data by the SMSS. The National ordinance protection of personal data does not, therefore, apply.

Article 14(1)(b) in conjunction with 14(4)
The party responsible for data processing is the natural person, legal entity or any other person who, or administrative authority that, alone or together with others, determines the objective of and the resources for the processing of (personal) data. A party responsible for data processing (such as a bank) is not required to provide the requested data to the service. However, if it decides to provide these data, the relevant rules laid down by or pursuant to ordinance do not apply to such provision.

Article 17(1)
Paragraph 1 provides an exhaustive list of the special powers of the SMSS. Observation and recording tools, as referred to in sub-paragraph a, may include cameras and binoculars. The tracking devices, locating equipment and recording tools that may be used in relation to the special authorisation to follow natural persons or goods include the deployment of radio beacons. The tapping, recording and listening in on conversations, telecommunications or electronic data transmission with the aid of technical tools (paragraph 1(e)) covers a wide range of 'tapping possibilities' due to its formulation as free of technology as possible; however, the deployment of a technical tool must be involved. Monitoring that does not require a technical tool is not designated as a special power. Paragraph 1(g) regulates the figure of the 'agent'. An agent of the service must be distinguished from an informant. An agent is a person who is deployed on the instructions and under the responsibility of the service to gather specific information or to promote or take measures; the latter is a form of actual action that may sometimes be necessary to protect the interests to be represented by the service in relation to national security. This then concerns, in particular, nipping certain anti-democratic activities or activities harmful to national security in the bud, with the ultimate aim of the prevention of the associated risks becoming a reality. An informant is a natural person who, due to his position or capacity, has access to or can access information that could be important for a service. However, the assistance for the performance of the tasks of the service by both an agent and an informant is provided on a voluntary basis.

Article 22
In view of the responsibility of the Minister of Telecommunication for the telecommunication policy of Sint Maarten, his consent is also required for tapping and recording of telecommunications, as well as the consent of the Minister responsible for the service (paragraph 1). The actual implementation of the authorisation to tap and record telecommunications requires that specific technical provisions must be realised by the concession-holder; in paragraph 2, an obligation to do so is imposed on him for that purpose.

Article 23
Article 23(1) contains a special provision to allow an agent to be provided with a (false) identity. Such a false identity is, among other things, required not to betray his true background, as well as for the agent's personal security. For operations under a false identity, the person concerned must be able to dispose of identity papers based on his false identity, for example. This all requires the cooperation of various administrative authorities. Specific provisions for this purpose are laid down in Article 23(1), involving a cooperation obligation for the administrative authorities concerned as well as provision for statutory provisions that could prevent such cooperation to be set aside.

Article 23(3) provides for the possibility that an agent may be charged (instructed) to perform actions that result in assisting in the committing of a criminal offence, or in committing of a criminal offence. Such an instruction may be issued only if this is necessitated by the proper performance of the tasks of the service or

the safety of the person concerned. The following may serve as an explanation. As part of the acquisition and retention of his information position, the agent will often have to perform certain activities, for example in order to win the trust of the relevant person or organisation. Partly in the interests of his own safety, he will have to conduct himself in such a way that there are no doubts about his reliability and credibility. In other words, he must conform as far as possible to the group behaviour pertaining in the relevant organisation. In particular cases, a situation may arise here in which the person concerned must aid and abet the committing of criminal offences, or commit criminal offences. In view of this, the agent may therefore receive instructions to that effect. However, in following those instructions, the agent may not, through his actions, incite another person to take different action concerning the plotting or committing of criminal offences than that to which that person's intent was already directed (paragraph 4). Incitement to commit criminal offences by the agent is not permitted.

Article 44(3)
On the basis of this paragraph, further rules will be imposed with regard to the way in which security investigations are conducted. If desirable, further rules may also be imposed, optionally, regarding the manner in which the information gathered in relation to the security investigation is recorded and the way in which the person concerned, by way of derogation from Article 34, could access that information.

Article 67
This Article regulates the relationship with the National accountability ordinance. A balance has been sought here between openness regarding the activities of the service and ensuring that the performance of the service is not undermined by this openness.

Paragraph 1 provides that the powers pursuant to the National ordinance General Audit Chamber relating to the service can be exercised only by the secretary or the chairman of the Audit Chamber. This limits the circle of knowledge-holders as far as possible. They may enlist the support of the head of the central internal accountant's service of Sint Maarten.

According to paragraph 2 Article 46(3) of the National accountability ordinance does not apply with regard to the incorporation of legal entities, as referred to in Article 17(1)(f). The purpose of paragraph 1 is that the intention of the Country to incorporate legal entities that are deployed for covert activities does not require notification of Parliament. In the Dutch Intelligence and security Services Act 2002 (Wiv), this is regulated in Article 21(8).

Article 70
Paragraph 1 lays down a regulation in the unlikely event that the service cannot (as yet) conduct any security investigations; this situation could arise in the period when the service is still being built up and the personnel and expertise required for the conduct of security investigations is not yet available (in full). In that case, the Minister, by agreement with the Minister of Justice, may address a request for support to one of the intelligence and security services within the Kingdom. If the relevant service responds to the request, security investigations will be conducted under the responsibility of the Minister and in compliance with the provisions laid down by or pursuant to the ordinance.

Paragraph 2 lays down a transitional provision for personnel employed by the NASS who may transfer to the SMSS as part of the transition.