Regulation on data processing in cases of discrimination on the BES-islands

On the proposal of the Minister of the Interior and Kingdom Relations of ... 2024, no. .../CZW/CZ;

Having regard to Article I, paragraph 5 of the Law on protection against discrimination on the BES;

Having heard the Advisory Division of the Council of State (advice of .... 2024, no. WO ...);

Having seen the further report of the Minister of the Interior and Kingdom Relations of .... 2024 no.... /CZW/CZ;

Have approved and understood:

Chapter 1. General

Article 1. Definitions

In this decision, the following definitions apply:

ADV BES: anti-discrimination facility in Bonaire, Sint Eustatius, and Saba that carries out the tasks as referred to in Article I of the law;

backoffice: anti-discrimination facility in European Netherlands that provides support and facilitation to the ADV BES;

visitor: natural person who physically or electronically contacts the ADV BES and requests support in cases of discrimination;

availability: the degree to which an information system is operational and accessible when an organization needs it;

front office: counter on the BES where the ADV BES provides its services;

information security: determining the necessary reliability of information processing and information systems to ensure confidentiality, availability, and integrity, as well as implementing, maintaining, and monitoring a coherent package of accompanying measures aimed at carrying out the tasks as referred to in Article I of the law;

information system: the collection of data, the associated individuals, processes, and software, as well as the implemented provisions for storage, processing, and communication for the purpose of carrying out the tasks as referred to in Article I of the law;

integrity: reliability, the degree to which an organization can rely on its information provision for its business and administrative processes;

personal data: any information relating to an identified or identifiable natural person, as referred to in Article 1, paragraph 2 under a., of the Law on the protection of personal data on the BES;

chain partner: organization outside the front office of the ADV BES and the backoffice, which contributes to or is professionally involved in the handling of reports of discrimination and the implementation of the tasks as referred to in Article I of the law, which refers or is referred to. This

includes a legal aid service, the police, the public prosecutor's office, social organizations (including organizations in the field of healthcare, welfare, and advocacy), and the College for Human Rights;

confidentiality: the degree to which access to and knowledge of an information system and the information therein are restricted to a defined group of authorized persons;

legal aid service: first-line legal aid service on the BES;

law: Law on protection against discrimination on the BES.

Chapter 2. Personal data

Article 2. Purpose limitation

The personal data as referred to in Article 4 shall not be used for other purposes and tasks as referred to in Article I of the law.

Article 3. Information and consent

1. The ADV BES:

a. informs a visitor about the processing of personal data;

b. requests consent for the processing of personal data if the visitor is a person as referred to in Article 4, under a.

2. If and to the extent that consent is not given, the ADV BES shall, where possible, provide support and record without processing personal data, taking into account the provisions of this chapter.

Article 4. Personal data in the ADV BES

In the ADV BES, the following personal data may be processed for the implementation of the tasks as referred to in Article I of the law and for the proper and reliable functioning of the information system:

a. about the visitor requesting help for themselves:

1° First name and surname;

2° Contact details, including postal address, email address, and telephone number;

3° Gender;

4° Nationality;

5° Date of birth;

6° Marital status;

7° Race and ethnic origin;

8° Political orientation or membership of a political organization;

9° Religion, belief, or membership of a religious or philosophical community;

10° Membership of a trade union;

11° Health condition;

12° Sexual orientation.

b. about the visitor requesting help for another:

1° First name and surname;

2° Contact details, including postal address, email address, and telephone number.

c. about the victim of discrimination who does not request help themselves: the data mentioned under a.

d. about the person who discriminates or would discriminate:

1° First name and surname;

2° Contact details, including postal address, email address, and telephone number;

3° Gender;

4° Relationship to the person discriminated against or who would be discriminated against;

5° Nationality;

6° Race and ethnic origin;

7° Political orientation or membership of a political organization;

8° Religion, belief, or membership of a religious or philosophical community.

e. about the contact person at a chain partner:

1° First name and surname;

2° Contact details, including postal address, email address, and telephone number.

f. about the handler:

1° First name and surname;

2° First name and surname of co-account holder(s) ADV-BES.

Article 5. Disclosure by the ADV BES

1. The ADV BES discloses the personal data referred to in Article 4 if and to the extent necessary for further handling and providing support in cases of discrimination, and if consent has been granted by the data subject as referred to in Article 4, under a and c, for the provision of their data, to:

a. the backoffice;

b. the relevant chain partner(s).

2. The ADV BES does not disclose personal data as referred to in Article 4 under a, b, and c to the person who discriminates or would discriminate without consent.

3. The ADV BES does not disclose personal data for reporting purposes.

Article 6. Retention periods

1. The ADV BES retains the personal data referred to in Article 4 for the duration of the implementation of the tasks as referred to in Article I of the law. The data are automatically deleted five years after the last necessary processing.

2. After forwarding, a request for cooperation, or a request for support, the ADV BES requests the relevant chain partner(s) and the backoffice to retain the personal data referred to in Article 4 for the duration of the handling and follow-up of the tasks as referred to in Article I of the law and to delete them no later than five years after the last necessary processing.

Chapter 3. Information security

Article 7. Security of personal data

In order to secure the personal data being processed and protect them against unauthorized or unlawful processing, as well as against loss, destruction or damage, the ADV BES takes appropriate technical, organizational and personnel measures, including measures concerning the proper and secure operation and use of information systems, access to and availability and integrity of information systems, and the detection and remediation of security breaches.

§ 3.1 Business Operations

Article 8. Information security policy

The ADV BES establishes a policy for the information security of the ICT systems used, including a security plan based on risk identification and risk assessment. The information security policy is a continuous process that is an integral part of the regular business management cycle and is reviewed and adjusted as necessary every two years.

Article 9. Organization and management

The ADV BES assigns tasks, responsibilities, and coordination regarding information security and implements appropriate management measures, including those related to the use of ICT systems and information processing.

Article 10. Personnel and physical security

The ADV BES equips its staff to implement the information security policy and protects spaces and equipment.

Article 11. ICT facilities and information systems

The ADV BES:

a. Ensures that privacy and security-enhancing measures are taken during the development of ICT, including data protection and security in the architecture, privacy-friendly default settings, and secure software;

b. Ensures the correct and secure operation and use of ICT facilities and information systems, including through the application of role separation;

c. Ensures the availability and integrity of ICT facilities and information systems, including through system planning, backup creation, and network management;

d. Implements access control measures for information and information systems;

e. Takes measures to detect and remedy security breaches, including vulnerability detection, incident reporting, response, escalation, damage control, communication, and evaluation.

§ 3.2 Monitoring and accountability

Article 12. Logging

1. In order to detect unauthorized information processing and system technical errors, the ADV BES maintains log files regarding the use of ICT facilities.

2. The log files include information on consulted files, login and logout times, and system technical data. This data is kept for a maximum of five years after the last necessary processing.

Article 13. Control

1. The ADV BES conducts a biennial audit of information systems. The audit focuses on network security, operating system, basic security, application security, and penetration testing.

2. Biennial reporting is done to the Minister. The report concerns the design and existence of security measures and procedures, and can also address the functioning of implemented management measures.

3. Based on a risk identification, the ADV BES develops improvement measures if the report indicates that certain aspects do not comply with the information security policy.

Chapter 4. Final provisions

Article 14. Entry into force

The articles of this decision come into effect at a time determined by royal decree, which may vary for different articles or parts thereof.

Article 15. Short title

This Decision shall be cited as: Decision on data processing in discrimination in the BES.

Given,

The Minister of the Interior and Kingdom Relations,

Explanatory Memorandum

Table of Contents

I General part

1 Reason

The draft law "protection against discrimination in the BES" aims to provide better protection against discrimination for the residents of Bonaire, Sint Eustatius, and Saba. Legislation and institutions are needed for this, just like they have been established and developed in the European part of the Netherlands in recent decades. The draft law achieves:

- Integral implementation of equal treatment laws in the BES;

- The establishment of a facility for each BES island that provides advice, information, registers complaints, and offers low-threshold assistance in discrimination matters: the Anti-Discrimination Facility BES (hereinafter: ADV BES);

- An adjudicative task at the College for Human Rights (hereinafter: CRM) regarding individual discrimination cases in the BES.

The draft law anchors the tasks of the ADV BES (Article I, second paragraph, of the law): support in handling complaints regarding discrimination as referred to in the relevant equal treatment laws, registration, advice, referral, mediation, and information. This could involve advising on possible steps to be taken by the reporting party and assisting in submitting a request for judgment to the CRM. The ADV BES processes personal data to the extent necessary for the proper execution of the mentioned tasks. Given the nature of the subject matter – often sensitive cases involving special personal data – and the scale of the islands, safety, reliability, and confidential treatment of complaints are essential. This is especially true when contact is made with, for example, discriminating employers, local goods or service providers, or chain partners in order to provide assistance to residents. Working with and possible integration into a legal aid service facility implies that an integral approach will be taken; here too, personal data will (have to) be exchanged. All of this requires careful protection of privacy and information security. Therefore, the law requires that rules be laid down by ministerial regulation regarding the data that is processed, to whom it is provided, how long it is stored, and how it is secured (Article I, fifth paragraph, of the law). This decision is intended to implement this.

2 Main points

This decision contains regulations for the processing, protection, and security of personal data by the ADV BES; the ADV BES is the addressee of this decision. In its work processes, which aim to provide assistance to residents of the BES who experience discrimination, both ordinary and special personal data are central. Personal data refers to all information about an identified or identifiable natural person (Article 1, second paragraph under a., of the Personal Data Protection BES Act). This means that information is either directly about someone or can be traced back to that person. In carrying out many tasks, the ADV BES involves some form of processing personal data (for example, in intake and registration of reports), often also data flows (for example, in consultation with the back office

and referral). The regulations in this decision are therefore related to the work processes and functionalities of the ADV BES. The ADV is a new facility for the BES.

In the European Netherlands, ADVs have been operating since 2009; the Municipal Anti-Discrimination Facilities Act stipulates that each municipality must establish a low-threshold, independent facility where citizens can file complaints about discrimination. This facility must be separate from the municipal organization to ensure independence. Therefore, ADVs can be found in all regions of the European Netherlands: often government-funded foundations, either as part of a joint arrangement or not, that provide physical offices where help and assistance can be sought for experienced discrimination. The ADVs are also accessible digitally. Furthermore, Discriminatie.nl operates, the national association through which the ADVs collaborate. Discriminatie.nl is responsible for promoting the quality and expertise of ADVs. The ADVs work with ADV-net: a technical provision (application) for registering complaints and reports, which also serves as the basis for the annual report. Employees record data case by case throughout the entire treatment process, from the first contact with a reporter to the closure of the file: who reports discrimination, which discrimination ground is applicable, on what area, what actions and follow-up steps are taken, to which chain partners referrals are made, etc. The use of ADV-net is supported by a manual for employees and a technical description. A privacy impact assessment (PIA) has been conducted, commissioned by Discriminatie.nl, to review the work process and security. ADV-net is ISO-certified (Kiwa).

On each BES island, the ADV will operate in a physical office, a front office, where a legal aid service may also be housed (in the future). This enables collaboration between professionals involved and ensures an approachable and integrated response to requests for assistance. The front office is expected to be in the form of a (government) foundation. There will also be a back office that provides support and facilitation to the ADV BES; the back office will be located in the European Netherlands. It is expected that Discriminatie.nl will be responsible for the setup and operation of the front office and back office of the ADV BES. The ADV BES will use ADV-net for its technical (ICT) support, as it is a usable, secure, and proven system that is well-suited for the work processes and functionalities needed in the BES. The ADV BES will also be digitally accessible. Inherent to carrying out the legal tasks of the ADV BES is the processing of typically special, very privacy-sensitive personal data. This decision sets rules on how personal data is processed by the ADV BES and obliges them (as the responsible party) to take legal, technical, and organizational measures. These regulations elaborate and fill in the BES Data Protection Act, in other words: they specify what applies to the ADV BES based on the BES Data Protection Act. Strictly legally, it is possible for ADV BES to operate based on (a combination of) consent from concerned individuals and de facto protective measures. There is, in short, no compelling need to establish legal rules. However, it was chosen to establish generally binding regulations. The BES Data Protection Supervisory Commission also insisted on this in its advice on the draft law "protection against discrimination in the BES." The generally binding regulations in this decision provide safeguards and legal certainty for residents of the BES who experience discrimination and clarity for chain partners and other parties involved. This way, additional protection is realized.

3 Ratio in relation to other regulations

As a result of the functioning of the ADV BES and the exercise of its legal tasks, personal data will be processed and exchanged; particularly within the BES (with chain partners, such as a legal aid facility and organizations in the field of health and welfare) but also with (the back office in) the Netherlands. In this context, the Wbp BES and the GDPR are relevant. This will be further elaborated on below.

The Personal Data Protection Law BES (Wbp BES)

With the introduction of the Wbp BES in 2010, the aim was to comply with the Constitution and establish an adequate level of protection for personal data on the three Caribbean islands. This includes a framework for the careful handling of (ordinary and special) personal data and the establishment of an independent supervisory authority, ensuring compliance with the standards. Legality of processing is essential; the Wbp BES prescribes purpose limitation (article 7), provides a regime for ordinary personal data (articles 8 onwards) and a stricter regime for special personal data (articles 16 onwards). Necessity and proportionality of processing, data minimization, and appropriate security measures are necessary. Personal data may be processed if the data subject has given explicit consent and if processing is necessary to comply with a legal obligation (articles 8 and 23). The Wbp BES also provides rights for the data subject such as access, legal protection, and oversight.

The (processing and provision by) ADV BES falls within the scope of the Wbp BES, as this law applies to automated or non-automated processing of personal data. This decision gives effect to the provisions of the Wbp BES. The privacy protection and information security regulations are tailored to the specific functionalities and tasks of the ADV BES, ensuring adequate protection and safeguards.

The chain partners are not the addressees of this decision. When they are involved in handling discrimination reports, refer to the ADV BES, or are referred to, they have an independent responsibility to comply with the Wbp BES. In this regard, the ADV BES also handles the relevant personal data very carefully (see chapter 2 of the decision). For the back office, compliance with the GDPR is required.

General Data Protection Regulation (GDPR)

The back office of the ADV BES is located in the Netherlands. Although the back office is technically connected to the ADV BES and is engaged by the ADV BES when dealing with personal data relating to residents of the BES, this decision assumes that the transfer of data from the back office to the ADV BES is subject to the GDPR. This aligns with the viewpoint of the Ctbp BES, which considers this data flow to the BES as a transfer to a third country, making Article 46 of the GDPR applicable. According to Article 46 of the GDPR, personal data may only be transferred to third countries, such as

the BES, if they have an adequate level of protection and data subjects have enforceable rights and effective remedies. This means the data exporter must assess whether the law of the BES guarantees adequate protection and provide additional safeguards if necessary. This assessment must be demonstrable for oversight purposes.

As indicated in point 2, Discriminatie.nl is expected to be responsible for the setup and operation of the back office in the Netherlands and the front office ADV in the BES. Compliance with the provisions of this decision is required for the ADV BES. These regulations pertain to privacy protection and information security and are tailored to the specific tasks, functionalities, and responsibilities of the ADV BES, providing safeguards and legal certainty for residents of the BES experiencing discrimination and clarity for chain partners and other stakeholders. This ensures compliance with the adequate level of protection required by Article 46 of the GDPR. Discriminatie.nl will ensure compliance with the requirements of this decision; the ADV BES will utilize secure and reliable (certified) technical facilities and professional, trained staff. See also below at point 4.

4 Content

This decision elaborates on Article I, fifth paragraph, of the law “protection against discrimination in the BES"; thereby also fulfilling the requirements of the Wbp BES. The provisions in the decision relate to privacy protection and information security and are tailored to the specific functionalities and tasks of the ADV BES. It is emphasized that for everything that is not regulated in this decision regarding privacy protection in the context of discrimination assistance, the provisions of the Wbp BES apply, such as regulations on transparency and the right of access and rectification. The various aspects of personal data protection related to this decision are further explained below.

4.1 Processing of personal data

This decision adopts the same principles as those underlying the Wbp BES: lawful processing, purpose limitation, proportionality and subsidiarity (data minimization), storage limitation, security, and integrity. A data protection impact assessment (DPIA) was carried out in preparation of the decision. This forms the basis for the provisions and explanation in the decision.

It should be noted for completeness that the protection of personal data is an ongoing and operational responsibility in practice. Privacy is not only protected by anchoring it in laws and regulations. This protection must take shape in practice and be able to evolve with the threats that arise over time and the protective measures that become available. The law and this decision regulate processing bases, retention periods, and disclosures that frame this responsibility, while also providing the flexibility to tailor the operational protection of personal data to the necessary and changing needs in practice.

4.1.1. Personal data in the ADV BES

Regarding proportionality – weighing the intrusion on privacy against the effects on citizens – the decision contains provisions to ensure that there is no further interference with the data subject's rights than necessary. The decision is the result of a careful balance between the importance of assisting with discrimination on one hand and protecting the personal privacy of residents of the BES on the other. This is reflected first and foremost in the fact that the processing of personal data is limited to the minimum data necessary and only to those data that are essential to the tasks of the ADV BES, to secure and maintain reliability.

Regarding subsidiarity – are there other ways to achieve the goal – an approach and design were chosen where the processing of personal data is minimal and with the least possible risks.

It is inevitable that personal data will be processed by the ADV BES; this is inherent to the core tasks of this service, which provides assistance and support in cases of discrimination (Article I of the law). This decision sets conditions for this processing. Firstly, the ADV BES must inform all visitors - in practice, also referred to as "reporters," but in reality, this is a more limited group - about the fact that personal data is processed by the ADV BES, what data (can) be processed, and that it is handled safely and meticulously. Additionally, the visitor requesting assistance and support is asked for consent to process their personal data. While obtaining consent is not strictly necessary for the performance of a legal task, as is the case here, this decision obliges the ADV BES to do so for additional privacy protection, given the sensitive nature of the matter and the importance of awareness.

If and to the extent that consent is not granted, the ADV BES will strive to carry out its tasks as effectively as possible without processing (all) personal data and will work with what is possible. For example, if the visitor/reporter consents to the processing of ordinary personal data but, because it is still sensitive, does not consent to the processing of special personal data, the ADV BES may still offer a listening ear, provide general information, or offer guidance. Such an initial step may lead to trust in this new service and to further contact with the ADV BES where the visitor feels free to share all relevant personal data. Anonymous reports of discrimination, where the reporter's personal data is unknown, can be recorded and included in the annual (policy) report. The ADV BES only processes the necessary data; what is necessary depends on the person whose data is being processed (reporter/victim, reporter/witness, perpetrator/opposing party, chain partner, ADV BES employee) and the circumstances of the case. For a visitor requesting assistance and support for themselves (victim), there will often be processing of one or more special personal data because it relates to the grounds of discrimination, such as race, sexual orientation, and/or disability or chronic illness. Only the data relevant to the specific case will be processed.

4.1.2. Provision by ADV BES

For the proper execution of legal tasks, it may be necessary for the ADV BES to involve the back office for support (such as guidance, advice, sharing of expertise) and/or request collaboration or follow-up action from one or more chain partners (such as referral to the police or a care institution). This involves the provision of relevant personal data if and to the extent necessary for the further handling and assistance with the relevant case, and if permission has been granted by the data subject.

Provision to a counterparty, such as a discriminatory landlord or provider of goods or services, can only be done with the consent of the data subject. For example, if mediation is being considered, data provision is unavoidable. This also applies when equal pay is demanded from an employer. In other words, a reporter or victim can remain anonymous to anyone other than the ADV BES; the case will then be treated confidentially. However, this does limit the available follow-up actions. Data subjects must be aware of this so that they can make an informed decision. Information provided by the ADV BES (article 3 of the decision) is helpful in this regard.

4.1.3. Retention periods

The retention period used by the ADV BES is five years after the last necessary processing. This period is derived from the maximum time needed for handling a request for help. The duration of a case varies depending on the circumstances. For example, when providing assistance in organizing and guiding a mediation process, initiating proceedings at the College, or supporting a legal case, there is a longer period of data processing compared to a brief oral advice given at the help desk. Nevertheless, even in the latter case, it is reasonable to retain data for longer than the duration of the contact, because experience in the European Netherlands shows that an initial contact is often followed by further consultations or follow-up processes and aftercare. After five years, the data is automatically deleted.

Chain partners and the back office are not the addressees of this decision. The decision does not provide 'hard' retention periods for them; they are responsible for their own data processing and data provision, and must determine their own retention periods, applying Article 10 of the Wpb BES and Article 5(1)(e) of the GDPR. Nevertheless, the decision provides that in the case of referral, a request for collaboration or support, the chain partner(s) and the back office are requested by the ADV BES to retain the relevant personal data for the duration of handling and follow-up of the task request, and to delete it no later than five years after the last necessary processing. The reason for this is that the purpose of the law and a proper execution of the tasks mentioned in it often require consultation between the ADV BES and one or more chain partners and/or the back office. The initiative for referral and collaboration often lies with the ADV BES. The retention period for chain partner(s) and back office is related to the time they need for follow-up; this also depends on work processes, processing times, and capacity. It is also difficult to provide a consistent norm due to the circumstances of each case. The College typically uses a five-year period, but the files that have led to a decision are kept longer and transferred to the National Archives. Although the regular tasks of chain partners and the back office align with those of the ADV BES, the anti-discrimination domain and the fact that they may have a - derivative - role in it are new subjects on which awareness needs to grow. For this reason, the decision provides for the ADV BES to alert on the issue of privacy protection.

4.2 Information security

The provisions in chapter 3 of this decision elaborate and concretize article 13 of the Wbp BES, which obligates the controller to take appropriate technical and organizational measures to secure personal data, taking into account the state of the art and the costs of implementation. These are regulations tailored to the specific tasks and functionalities of the ADV BES in terms of business operations and monitoring/accountability. The reason for this 'translation' is to provide clarity and legal certainty. This is desirable given the nature of the subject matter; it concerns new legislation and a new facility, the implementation of fundamental rights (non-discrimination, privacy protection), all within the context of the unique characteristics of the islands and the sensitive issue of discrimination.

The regulations pertain to the primary process; the processing of personal data and the associated security are inherent to the task of the ADV BES.

The information security provisions are performance obligations. With their structure and formulation, a balance is struck between, on the one hand, being normative and verifiable (providing guidance) with respect to the security within and transmission within the facility, and, on the other hand, allowing flexibility. This enables the ADV BES to tailor its approach (risk-based management) to suit the structure of its task performance. This approach upholds the system responsibility of the Minister of BZK and the responsibility that the ADV BES holds for its own business operations. Future collaboration between the ADV BES and a legal aid facility in the front office will not change this. If both offer their services at the same physical location, they use their own systems and must comply with the regulations that apply to them. An integrated approach to assistance requests does not mean that ICT, files, registration, etc. are linked. However, measures related to management and personnel and physical (access) security must be coordinated.

It is especially important that the decision mandates data protection by design (privacy by design) and by default settings (privacy by default). The former involves attention to data protection in the design phase of a product or service (privacy enhancing technologies). The default settings should also be as privacy-friendly as possible. Both principles are mandatory under the AVG when processing personal data. This is not the case under the Wpb BES; the provisions of this decision, which nonetheless align with and serve as an elaboration of article 13 of the Wbp BES, thus provide an extra safeguard under the BES. Security should also be integrated from the development process (security by design). This means that security measures are built into the architecture, design, and code of the software. Additionally, measures regarding data storage and access and use by employees are important, such as two-factor authentication for logins and restricted access to individual files.

5 Supervision and enforcement

The Data Protection Supervisory Commission BES (Ctbp BES) has the task as an independent supervisor to oversee compliance with the provisions of the Wbp BES (Article 44 Wbp BES). Oversight of the processing of personal data as regulated in this decision, which elaborates and concretizes the Wbp BES, also falls within the authority of the Ctbp BES. The Ctbp BES is authorized, in accordance with Title 5.2 of the General Administrative Law and Sections 5.3.1 and 5.3.2 of the General Administrative Law, to impose an order subject to administrative enforcement or a penalty payment order to enforce the obligations imposed by or under the Wbp BES (Article 51 Wbp BES). See point 7 for the advice issued by the Ctbp BES regarding this decision.

Furthermore, the decision obligates the ADV BES to monitor and be accountable for the security of the processing. There is a requirement for logging: recording data on the use of ICT in order to enable the verification of its correct functioning. This way, transactions can be checked and incidents can be managed. The ADV BES must also assess its information security policy. This is done by examining the security process and the (technical) information systems. The report prepared on this basis is part of the regular accountability of the ADV BES and must also be submitted to the minister every two years. This allows for an assessment of whether the ADV BES meets security requirements, whether there have been any shifts, improvements, or deteriorations compared to previous years, and whether improvement measures are needed. It is reasonable to link this accountability to the reporting obligation of the ADV BES regarding registered complaints and notifications (Article I, second paragraph, under b, of the law).

6 Consequences and Feasibility

This decision contains regulations for a new provision for Bonaire, Sint Eustatius, and Saba, the ADV BES, which will operate within new local facts and circumstances (insular uniqueness). Each of the islands will have to comply with the regulations regarding the processing of personal data and information security. The ADV BES will operate on each island in a physical office, a front office. There will also be a back office, stationed in European Netherlands, providing support and facilitation to the ADV BES. Although it is a new provision, it will be set up as much as possible using proven techniques and processes that seem suitable for use in the BES. The starting position therefore seems usable and workable. Discrimination.nl is expected to be responsible for the setup and operation of the front office and the back office. This includes staffing, organization, housing, and technical (ICT) support (ADV network). The ADV BES bears the administrative burdens and costs as the responsible party; structural funding is provided from the budget of the Ministry of the Interior and Kingdom Relations. It is expected that this decision is feasible for Discrimination.nl, as the practices used in European Netherlands align with the regulations in the decision; the subject matter is not new, experience has been gained in European Netherlands, so the regulatory burden for the ADV BES is expected to remain limited. However, unlike in European Netherlands, in the BES, there will be public law framing by legal binding and enforceable regulations. This leads to greater awareness regarding the necessity and design of privacy protection, legal certainty, and legal protection for individuals.

7 (Internet) consultation and issued advice TBA

During the (internet) consultation, which ran from ... to ..., 2024, the following responses were received.

Data Protection Supervision Committee BES (Ctbp BES)

Advice was received during the (internet) consultation.

The Ctbp BES notes that ...

It is advised to...

In response to this, the following is noted.

Advisory Committee on Administrative Burden (ATR)

Advice was received during the (internet) consultation.

The ATR notes that ...

It is advised to...

In response to this, the following is noted.

Other

Includes:

Public bodies Bonaire, St. Eustatius, and Saba

Chain partners / social organizations in the BES

NCDR

National Ombudsman

II Article-by-article explanation

Article 2. Purpose limitation

This article specifies, in accordance with article 7 of the Wbp BES, that the ADV BES does not use personal data for other - in this case legally anchored - purposes and tasks as referred to in article I of the law. Specifically, this involves providing independent support for discrimination: a. support to individuals in resolving their complaints regarding discrimination as referred to in the designated equal treatment laws, b. registration of discrimination complaints and annual reporting on the matter, c. advising on possible steps to take, d. referral to other support services, e. mediation, and f. information provision and education.

Article 3. Information and consent

Although the tasks of the ADV BES involve data processing - assistance with discrimination is not possible without processing a minimum of personal data - as many safeguards as possible are implemented for necessary, proportionate, and secure processing, by legally regulating processing (including disclosure) and attaching strict conditions to it.

In this regard, paragraph (a) of the first paragraph specifies that the ADV BES, as the responsible party under article 1, paragraph 2, under d, of the Wbp BES, must inform all visitors (whether as victims themselves or witnesses of discrimination against others) that the ADV BES processes personal data, what data they are, and that it is handled safely and carefully. The purpose of this is to make visitors aware that the ADV BES, in order to do its work optimally, will often have to process special personal data related to grounds for discrimination that are sensitive in the island communities. For data processing necessary to comply with a legal obligation to which the responsible party is subject, consent from the individual whose personal data it concerns is not necessary (article 8, paragraph c, Wbp BES). However, paragraph (b) of the first paragraph requires the ADV BES to request consent from the visitor who makes a report as a victim for the processing of their personal data. This should be considered an additional safeguard, given the sensitive nature of the matter and the desirability of awareness. Personal data of other parties, such as those who act or would act discriminatorily (for example, an employer or a hospitality establishment), are processed without consent. The legal basis for this processing is - in accordance with article 8, paragraph c, Wbp BES - this decision.

The second paragraph makes it clear that if consent is not granted, this must be respected. The ADV BES will then consider what is possible; it is an obligation to make efforts to do something for the visitor within the limitations. Registration of discrimination (facts, circumstances, grounds) will generally be possible; no personal data is required for this. It must be borne in mind that equal treatment legislation, and the resulting rights, obligations, and institutions, are new in the BES. Residents, businesses, and organizations must get used to the new facility of ADV BES, the fact that experienced discrimination can be reported, help and assistance can be obtained, and a report may sometimes have a significant follow-up. For example, if the visitor/the victim consents to the processing of ordinary personal data but, because it is (still) sensitive, not to special personal data, a listening ear, general information, or some guidance may still be provided. Such an initial step may lead to trust in this new facility and further contact with the ADV BES where the visitor feels free to

share all relevant personal data. This matter involves a careful process of development that needs to be carefully shaped.

Article 4. Personal data in the ADV BES

This article specifies, in connection with article 11 of the Wbp BES, which data are effective and proportionate to carry out the tasks of the ADV BES and - consequently - to ensure the reliable operation of the registration system. The ADV BES does not process all personal data listed in this article in every case, but only those data that are necessary; what is necessary depends on the circumstances of the case. Therefore, Article 4 uses the term "may". Article 4 contains an exhaustive list.

The ADV BES processes only the data that are necessary; what is necessary depends on the person whose data it concerns and the circumstances of the case. In the case of a visitor requesting help for themselves, as a victim of discrimination, there will often be processing of one or more special personal data because the discrimination grounds are related, such as race, sexual orientation and/or disability or chronic illness. Only the relevant data for the specific case are processed.

Depending on the circumstances of the case, a large number of regular and special personal data may be processed regarding the visitor requesting help for themselves (a). This also applies to a victim who does not approach the ADV BES themselves, but for whom a witness or advocate requests help. In this case, since the visitor - often referred to as the "reporter" in practice - provides personal data of another to the ADV BES, the consent of the person whose data it concerns is not obtained. The legal basis for this processing is - in accordance with article 8, under c, Wbp BES - provided in this decision (c). Only a few regular personal data are processed regarding the visitor requesting help for another (witness or advocate). This also applies to the professionals in the ADV BES (treatment provider and their substitute/co-custodian) and the contact person at a chain partner, such as a police officer or healthcare provider. To obtain a comprehensive understanding of the case, it is necessary to process some special personal data of the person acting discriminatorily or potentially acting discriminatorily (perpetrator, opposing party).

Article 5. Disclosures by the ADV BES

The disclosure of personal data through transmission or transfer is a form of processing, as stated in article 1, second paragraph, under b, of the Wbp BES. For clarity and alignment with regular work processes, the processing (article 4) and disclosure (article 5) of personal data are regulated in separate provisions. It is emphasized that processing and disclosure by the ADV BES serve the same purpose: providing assistance and support in cases of discrimination. This does not involve "further processing" within the meaning of article 9 of the Wbp BES, which refers to processing for a purpose other than the original purpose for which the personal data were collected.

Article 5 specifies in the first paragraph that the ADV BES may disclose personal data to the back office and the relevant chain partner(s), if and to the extent necessary for further processing and providing assistance in cases of discrimination. In order to do so, consent must be granted by the victim concerned; no further action is taken on a report without their knowledge and consent. It is

difficult to imagine, for example, that the police or a healthcare or welfare institution would provide assistance to a victim against their will. This is different when it comes to the processing and disclosure of data concerning the perpetrator of discrimination; the legal basis for this processing is provided in this decision. The same applies to disclosures to the back office. The fact that the back office - which is not the addressee of this decision - may technically be part of the ADV system does not mean that access can automatically be obtained to the contents of BES files and the personal data contained therein. Following through on a request for expertise or support requires an active action by the ADV front office employee and, when it comes to the personal data of the victim, their consent.

According to the second paragraph, the ADV BES does not disclose personal data as referred to in article 4, paragraphs a, b, and c to the person acting discriminatorily or potentially acting discriminatorily (opposing party) without consent. As outlined above in 4.1.2, this can hinder further actions in certain cases, as disclosure of personal data is essential for actions such as mediation or a claim for damages.

According to the third paragraph, the ADV BES does not disclose personal data for reporting purposes. Reporting - a task based on article 1, paragraph 2, under b, of the law - serves a purpose of accountability and policy and is not intended to enable individual assistance, but rather to provide local information, for which general (statistical) data may suffice. It should be noted that even if no personal data are used for registration and reporting, in a small community there may still be (perceived) identifiability. This must be handled with caution.

Article 6. Retention periods

In accordance with article 10 of the Wbp BES, personal data are not kept longer than necessary for the realization of the purposes for which they are collected or processed. Article 6 of this decision elaborates on this, tailored to the tasks and work processes of the ADV BES. The retention period of five years is related to the maximum time needed for the handling of a case. The processing time varies depending on the circumstances of the case, including the nature and complexity of the discrimination and the necessary cooperation with a chain partner. See also 4.1.3.

Article 7. Security of personal data

This article is an introductory ('umbrella') provision, which is elaborated in the following provisions of the decision concerning the design and management (system) of information security. It is also referred to as information security, to emphasize the necessary continuity and cyclical nature. The provisions concretize article 13 Wbp BES, which obliges the controller to take appropriate technical and organizational measures to secure personal data, taking into account the state of the art and the costs of implementation. Articles 7 and following contain regulations tailored to the tasks and functionalities of the ADV BES in terms of management and monitoring/accountability.

Article 8. Information security policy

The ADV BES is responsible for its own primary process. This involves the use of ICT: information systems, telecommunications, and computers. The starting point here is risk management: to achieve the correct security of information (systems), a risk-based approach must be taken. This means that risks must be identified, assessed and manageable in a systematic manner. The ADV BES makes a conscious assessment and must responsibly manage risks, with the weighting factors also aimed at consistency and the overall safety. Inherent to risk-based business operations is that the outcomes of a risk analysis and the measures to be taken (including accepting residual risks) are customized. The information security policy and the measures to be taken in that regard must at least include the aspects indicated in the following articles.

Articles 9 (Organization and management) and 10 (Personnel and physical security)

Information security must be organized and managed. Tasks, responsibilities, and coordination must be assigned and control measures must be taken, including regarding the use of assets such as computers and mobile devices. There is room for interpretation in the implementation; the measures must fit the risk profile of the ADV BES. The same applies to personnel management and security of the (physical) environment. Control measures include, for example, screening and training (security awareness) of employees. Logical and physical (access) security and security of equipment may include the use of a safe, firewalls, network segregation (separation of networks), authorization (which employee has access to what), linking accounts to individuals (so that multiple people cannot use the same account), and working with access rights.

Article 11. ICT facilities and information systems

This article provides for concrete measures to be taken by the ADV BES, including embedding data protection and security in the design phase (privacy by design and security by design), privacy-friendly default settings (privacy by default), secure access and use of ICT, continuity and recovery of security breaches. This includes keeping software up to date (such as browsers, antivirus software, and operating systems), making backups (to ensure the availability and access to personal data can be restored in a timely manner), regularly testing security, and establishing internal rules for handling data breaches and incidents. It is also important to separate tasks that pose a risk of misuse, unauthorized or unintended access to information and assets (segregation of duties). This ensures that an individual employee cannot influence the entire process. It is also crucial that personal data is not exchanged in contacts via Facebook – commonly used in the BES –, Messenger, WhatsApp, etc.

Ideally, all security measures taken should be part of a (strategic) action plan aimed at the long-term development of the entire organization (system planning).

Article 12. Logging

To detect unauthorized information processing and system technical errors, the ADV BES must keep log files and regularly check them. Logging includes accessed files, login and logout times, and system technical data. The storage period of five years aligns with the storage period for personal data (Article 6). After five years, the log data is automatically deleted.

Article 13. Control

In order to enable the Minister of BZK to exercise his (system) responsibility, the ADV BES must assess its information security policy. This is done through an inspection of the information systems, resulting in a biennial report prepared by the ADV BES. The report based on this inspection should be part of the regular accountability (planning and control cycle) and should also be submitted to the minister biennially. For reasons of feasibility, the focus of the inspection is on the (technical) ICT facilities and the associated management processes. The potential outsourcing of (parts of) the inspection does not diminish the responsibility of the ADV BES. If the report shows that certain aspects do not comply with the information security policy, the ADV BES must take corrective measures.

Article 14. Entry into force

It is important that privacy protection within the ADV BES is in order when applying equal treatment legislation in the BES. Therefore, this decision is expected to enter into force simultaneously with the law.

The Minister of the Interior and Kingdom Relations,

J. J. M. Uitermark