Authority for Personal Data

PO Box 93374, 2509 AJ The Hague

Bezuidenhoutseweg 30, 2594 AV The Hague

T 070 8888 500 - F 070 8888 501

authority data.nl

Confidential/Registered

Minister of Foreign Affairs

Mr W.B. Hoekstra MBA

Rhine Street 8

2515 XP The Hague

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

Contact

[CONFIDENTIAL]

Topic

Decision to impose a fine and an order subject to periodic penalty payments

Dear Mr Hoekstra,

The Dutch Data Protection Authority (AP) has decided to inform the Minister of Foreign Affairs (hereinafter: the Minister) to impose an administrative fine of € 565,000. The AP has come to the conclusion that the Minister, as controller in the process of granting so-called Schengen visas,

insufficiently inform data subjects and the security of the processing of personal data

insufficient guarantees. With regard to the security of personal data, the AP has with regard to

in short, the New Visa Information System (NVIS) has determined that:

a security plan is missing;

insufficient measures have been taken (or taken) to physically protect personal data;

-

-

- incomplete procedures exist regarding (control of) access rights to NVIS;

-

there are shortcomings in the log files and their regular checks; and

- the procedure for reporting security incidents was incomplete.

As a result, the Minister is acting in violation of Article 13, paragraph 1, under e, and Article 32, paragraph 1, of the General Data Protection Regulation (GDPR). The AP has decided to also issue you an order subject to a penalty to impose, which concerns the rectification of these violations - which in determining this decision has not yet been completed.

The AP explains the decision in more detail below. Chapter 1 is an introduction and chapter 2 contains the findings. Chapter 3 elaborates on the (level of the) administrative fine and Chapter 4 states: the order subject to penalty. Finally, Chapter 5 contains the operative part and the remedies clause.

1

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

Content

2. Findings

2.1 Processing personal data

2.1.1 Actual findings

2.1.2 Legal Assessment

2.2 Controller and processor(s)

2.2.1 Factual Findings

2.2.2 Legal assessment

2.3 Security plan NVIS

2.3.1 Legal framework

2.3.2 Actual findings

2.3.3 Legal Assessment

2.4 Physical security access to NVIS

2.4.1 Legal framework

2.4.2 Factual Findings

2.4.3 Legal Assessment

2.5 Access rights to NVIS and personnel profiles

2.5.1 Legal framework

2.5.2 Actual findings

2.5.3 Legal Assessment

2.6 NVIS Usage Monitoring: Log Files

2.6.1 Legal framework

2.6.2 Factual Findings

2.6.3 Legal Assessment

2.7 NVIS Usage Control: Security Incidents

2.7.1 Legal framework

2.7.2 Factual Findings

19

22

25

25

26

32

36

36

37

40

42

42

44

47

48

48

48

49

50

51

2/64

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

3 Fine

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

1 Introduction

1.

2.

3.

4.

1.1 Background

The AP is responsible for supervising the national part of a number of European countries information systems, including the Visa Information System (hereinafter: VIS) and the Schengen Information System (hereinafter: SIS II). Under the EU legal framework of these systems, the AP independently monitor the lawfulness of the processing of personal data by the Member State concerned, including transmission to and from the central European facility of VIS and SIS. For visa applications, access to the European VIS takes place through a national system, te know: N.VIS. The specific application that falls under N.VIS and by the Ministry of Foreign Affairs (hereinafter: BZ) is used for Schengen visas, the New Visa Information System (hereinafter: NVIS).

The NVIS contains the application data, including biometric data, of all applicants who Dutch consular post abroad want to obtain a Schengen visa for the purpose of their stay in the Netherlands and/or in other Schengen countries. Applications for Schengen visas are made in countries outside the Schengen area and where there is also no special visa exemption. At the processing of visa applications, it is also always checked whether the applicant is listed in SIS II. SIS II includes alerts entered by Member States in the field of, among other things, European arrest warrants and declared undesirable. The SIS II check takes place automatically, in the background of a

visa application through NVIS.

In 2015, the Schengen evaluation took place, in which the supervision carried out by the AP on the national part of the SIS II and VIS was assessed. The 2015 Schengen evaluation report explicitly states included that the AP must carry out regular checks at the Dutch consular posts. This one AP checks are also part of the police and judicial multi-year plan that the AP follows in the context of of its supervision of, inter alia, the aforementioned SIS II and VIS (systems).

As a result of this, the AP conducted a supervisory investigation at BZ and a number of parties who have a role in the process of granting Schengen visas. The study included the following organizations:

- the Dutch embassy in London, United Kingdom (hereinafter: consular post in London);
- the Dutch embassy in Dublin, Ireland (hereinafter: consular post Dublin);
- the Consular Service Organization in The Hague, which acts as the back office of the
-
-
-

visa granting (hereinafter: the CSO);

[CONFIDENTIAL] (hereinafter: Processor 1) in London, United Kingdom, acting as external service provider (hereinafter: EDV) in the visa process of the consular post London;

[CONFIDENTIAL] (hereinafter: Processor 2) in Utrecht, the executor of various IT tasks in relation to the national visa information system; and

[CONFIDENTIAL] (hereinafter: Processor 3) in Amsterdam, the service provider for the NVIS servers.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

1.2 Purpose of research

The investigation of the AP focused on the (selected) physical, organizational and technical security aspects of NVIS in the context of the Schengen visa process and included the security plan, physical security, granting access rights to NVIS and logging the NVIS usage. In addition, compliance with legal requirements was checked with regard to the information provision to visa applicants and the training of staff involved in the visa process.

1.3 Visa Process for Short Stay Schengen Visa

In this section, the AP provides an explanation of the Schengen visa process in general, and specifically with regard to the consular posts in London and Dublin.

5.

6.

Schengen short stay visa

A short-stay visa is called a "Schengen Visa". With this visa, persons within a period of 180 days, staying in the Schengen area for 90 days.1 With a Schengen visa it is – short in summary – for a person without EU nationality allowed to travel freely within 26 Schengen countries. The country where someone has to apply for the visa is determined by the main purpose of the applicant's journey or main destination.

The visa process at the examined consular posts consists of the following steps1:

7.

[CONFIDENTIAL]

1.

[CONFIDENTIAL]

2.

[CONFIDENTIAL]

3.

[CONFIDENTIAL]2

4.

5.

[CONFIDENTIAL]

6. [CONFIDENTIAL]3

7.

[CONFIDENTIAL]

8. [CONFIDENTIAL]

9. [CONFIDENTIAL]

8.

After the registrations have been completed and the substantive steps have been completed, a decision can be made on the visa application are taken. This decision is registered in NVIS.4 In the event of a positive decision the visa sticker is printed and pasted in the passport of the applicant, in the event of a negative decision, issued a refusal order. In both cases, the decision is registered in VIS.5

1 File 3, appendix 1: NVIS Visa Application Processing Manual February 2018, p. 19.

2 When processing visa applications, it is also always checked whether the applicant is listed in the SIS II system. SIS II includes alerts introduced by member states on, among other things, the field of European arrest warrants, and unwanted aliens. The SIS II control takes place automatically, in the background of a visa application via NVIS.

3 File 3, Appendix 3: Visio-Schengen Flowchart, p. 6 and 7.

4 File 3, appendix 3: Visio-Schengen Flowchart, p. 7.

5 File 3, appendix 3: Visio-Schengen Flowchart, p. 9.

Date

[CONFIDENTIAL]

9.

10.

11.

12.

Apply for a Schengen visa at the consular post in London

The Consular Post in London works together with Processor 1 who fulfills a role of an EDV6. The tasks7 of the EDV include, among other things:

[CONFIDENTIAL]

Processor 1 handles the intake of most visa applications that go through the London consular post.

In the context of a visa application, the applicant downloads the application form via the BZ website or via the website of Processor 1. The applicant then makes an appointment with Processor 1 via the appointment system of Processor 1. On the day of the appointment, the applicant reports to Processor 1.

Processor 1 successively performs the following tasks:8

[CONFIDENTIAL]

The consular post in London carries out the following tasks, among others:

[CONFIDENTIAL]

The tasks of the CSO include the following activities:9

[CONFIDENTIAL]

6 Consideration 13 Visa code, Article 40 paragraph 3 Visa code, Article 43 Visa code.

7 Article 43(5) Visa Code.

8 File 3, Appendix 3: Visio-Schengen Visa Flowchart.

9 File 3, appendix 3: Visio-Schengen visa Flowchart, p. 4-5.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

13.

14.

15.

16.

17.

In some cases, submitting an application to the Immigration and Naturalization Service
(IND) necessary or is it necessary to consult or inform Member States.10 In addition, it may be
necessary to interview the applicant.11 When processing visa applications,
always checked whether the applicant is listed in SIS II. The SIS II check takes place automatically, in the
background of a visa application via NVIS. After these steps have been completed, a decision can be made on the
visa application are taken. This decision is registered in NVIS.12 In the event of a positive decision
the visa sticker is printed and pasted in the passport of the applicant, in the event of a negative decision,
issued a refusal order. In both cases, the decision is registered in VIS.13

Applying for a Schengen visa at consular post Dublin

The Dublin consular post operated during the AP's investigation without the intervention of an EDV and
handles visa applications itself. Hereby largely the same steps of the
visa application process followed as with Processor 1 and the London Consular Post. [CONFIDENTIAL].
[CONFIDENTIAL]. In the context of a visa application, the applicant downloads the application form
via the website of the embassy or BZ. An appointment for an intake at the consulate can be made
are posted on the embassy's website via a link to an appointment system.

As part of the visa process, the consulate performs the following tasks, among others:

[CONFIDENTIAL]

In its role as back office, the CSO performs the same tasks as those in the case of the consular post London. In addition, the CSO has an important task in registering the visa application data which occupies the consular post Dublin and as paper files sent by post to the CSO in The Hague sends.

BZ's view

BZ has stated that since the investigation by the AP there have been some changes to the above visa process have been made. Processor 1 currently takes live photos, and the intake of the visa applications no longer goes by post (via the consular post in London). In addition, consular post Dublin now use an EDV.14

10File 3, appendix 3: Visio-Schengen visa Flowchart, p. 6.

11 File 3, appendix 3: Visio-Schengen visa Flowchart, p. 7.

12 File 3, appendix 3: Visio-Schengen visa Flowchart, p. 7.

13 File 3, appendix 3: Visio-Schengen visa Flowchart, p. 9.

14 Written Opinion BZ of 15 October 2021, p 3.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

18.

19.

20.

1.4 Legal framework

For the legal framework, the AP refers to ANNEX 1.

1.5 Process

In the context of this investigation, the AP used various investigation methods. The AP performed

desk investigation, requested information in writing and has several locations at various locations

on-site investigations (hereinafter: OTPs). During the OTPs, the inspectors of the AP

conducted interviews and researched the information systems used in the

visa process. As a result of the OTPs performed, the AP has provided the additional documentation

requested and written questions. Several files were requested during the research

relating to the granted access rights to NVIS, NVIS logging and selections from the NVIS

databases (in particular tables of the databases).

In a letter dated 13 August 2021, the AP sent the Minister an intention to enforce. The

On 15 October 2021, the Minister provided a written opinion on this intention and the consequences thereof

underlying report with findings.15 On November 4, 2021, the AP has a

opinion session took place during which BZ also explained its opinion orally.16 On 10

In December 2021, the Ministry of Foreign Affairs sent further documents upon request.17

15 Written Opinion BZ of 15 October 2021.

16 Letter from the Ministry of Foreign Affairs to AP dated 19 November 2021 with appendix 1 Interview report.

17 E-mail BZ to AP dated 10 December 2021.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

2. Findings

21.

22.

23.

24.

2.1 Processing personal data

2.1.1 Actual findings

The Visa Code specifies which data the Member States must collect in order to be able to apply for visas provide. It is laid down in the VIS Regulation that the following data for the benefit of the processing and taking decisions on visa applications for the Schengen area in the VIS should be stored: alphanumeric data concerning the applicant and the requested, visas issued, refused, annulled, revoked or extended, a photo of the applicant, fingerprint data and links to other applications.18 Upon receipt of an application, the visa authority to update the application file without delay by entering different data in the VIS, such as first and last name, gender, place and country of birth, nationality, type of visa issued requested, purpose of the trip, place of residence, current profession, photo and fingerprints of the applicant.19 Authorized staff of the visa authorities have access to the VIS and can enter, change or delete data.20 For example, when a visa is issued, when a visa application, in the event of a refusal of a visa application, in the event of annulment/revocation of a visa or a visa extension21 data added to the application file. Then it is it is possible that the data will be changed or deleted during the application process.22 BZ (and its consular posts) use the NVIS in which personal data for the benefit of the Schengen visa process will be saved, modified and deleted.

2.1.2 Legal Assessment

The data of visa applicants that are processed in the NVIS qualify as personal data in the sense of Article 4(1) of the GDPR, as it concerns information about identified natural persons.23 A part of this data is biometric data within the meaning of Article 4(14) and Article 9 GDPR and thus qualify as special personal data.

Furthermore, entering, consulting, storing, viewing and changing personal data in NVIS falls under the scope of the concept of processing of personal data within the meaning of Article 4(2) of the GDPR. the AP notes that personal data is processed by means of the NVIS when going through the short stay visa process.

18 Article 5(1) Regulation (EC) No. 767/2008 of the European Parliament and of the Council of 9 July 2008 on the Visa Information System
(VIS) and the exchange of information between Member States in the field of short-stay visas ('VIS Regulation'), OJ 2008, L218/60.

19 Article 8, paragraph 1 jo. 9 VIS Regulation.

20 Article 6(1) VIS Regulation.

21 Articles 10 to 14 VIS Regulation.

22 Articles 24 and 25 VIS Regulation.

23 Because, among other things, name and address details and also the citizen service number are processed, the identity of the persons is established and therefore concerns
identified persons.

Date
February 24, 2022

Our reference
[CONFIDENTIAL]

25.

26.

27.

28.

2.2 Controller and processor(s)

2.2.1 Factual Findings

Ministry of Foreign Affairs

The AP has established that for the Netherlands the Minister of Foreign Affairs is the designated person responsible for processing of personal data in the VIS.24

The AP has established that an important part of the tasks in the field of NVIS services

is organizationally assigned to the Directorate-General for European Cooperation.25 Under this Directorate a number of directorates, two of which have a particular role in issuing visas.

Firstly, the Consular Affairs and Visa Policy Department (DCV). DCV is, among other things, responsible for the providing consular services to Dutch nationals abroad and directing the consular function in the department and on the missions.26Secondly, the Consular Service Organization (CSO) in The Hague. CSO is a shared service organization whose primary task is to provide back-office processes related to the issuance of visas and travel documents. The AP has established, and the Ministry of Foreign Affairs has confirmed this, that the back office of the consulate in London and the consulate in Dublin is located at CSO. In addition, CSO takes care of the back office activities with regard to a number of other consular services and products.27

Processor 1

Processor 1 is an outsourcing and technology services company that operates in various countries for the Netherlands executive matters related to visa and passport issuance. The head office, [CONFIDENTIAL] is based in Dubai, United Arab Emirates.

Processor 1 has been designated as an external service provider28 to facilitate visa application facilities. It The company is setting up physical visitor centers where those involved can submit their applications. In London Processor 1 for BZ provides the front office for the visa applications submitted in the United Kingdom be submitted. With regard to this work, on March 21, 2019, a concession agreement concluded between Processor 1 and BZ.29 Pursuant to this assignment, Processor 1 Process visa applications and biometric information. Employees of Processor 1 take this information received from the applicant. At the [CONFIDENTIAL] location in London, ICT facilities made [CONFIDENTIAL].30 Processor 1 does not have access to NVIS, this happens at the CSO. At Processor 1, applicants can hand in and collect their passports.

24 List of competent national authorities whose duly authorized staff have access to the Visa Information System (VIS) to enter, modify, delete or consult data (2012/C79/05).

25 Article 7(2)(d) Foreign Affairs Organizational Decree 2019.

26 Article 7(2)(c) Foreign Affairs Organization Decree 2019.

27 Article 7(2)(d) Foreign Affairs Organizational Decree 2019.

28 Article 40(3) Visa Code.

29 File 3, appendix 4a: [CONFIDENTIAL].

30 File 3, appendix 4d: Appendix 1 to the standard contractual clauses.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

29.

30.

31.

32.

33.

34.

35.

For the transfer of processed personal data by BZ to Processor 1, a

arrangement made on the basis of the regulations issued by the European Commission, in accordance with Article 46(2)(c) of

the GDPR

established standard contractual clauses for data protection (´Standard Contractual

Clauses´).31 Article 1, sub b and c, states the following:

(b) ´the data exporter´ means the controller who transfer the personal data;

(c)´the data importer´means the processor who agrees to receive from the data exporter personal data intended for

processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not

subject to a third country´s system ensuring adequate protection within the meaning of Chapter V of Regulation (EU) 2016-679.

Article 4 of the Standard Contractual Clauses contains obligations laid down by the 'data' exporter´. Pursuant to Article 4(b) of the Standard Contractual Clauses, the 'data exporter' undertakes to the obligation ‘that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses'.

Appendix 1 to the Standard Contractual Clauses states that BZ is the 'data exporter' and [CONFIDENTIAL] the ´data importer´.32

Processor 2

The investigation of the AP has shown that Processor 2 fulfills an important role within the visa granting process. Processor 2 is a consultancy company that focuses on advising and supplying of information technology.

The services provided to NVIS are provided by the following organizational units of Processor 2 performed: [CONFIDENTIAL] as part of [CONFIDENTIAL] and [CONFIDENTIAL].

[CONFIDENTIAL] (and therefore Processor 2 Nederland BV) uses the services of the [CONFIDENTIAL] in India which is part of Processor 2 [CONFIDENTIAL].33

Processor 2 entered into an agreement with BZ on August 31, 2010 for the supply of support services for NVIS. The service includes the application and technical management, making available (including hosting), maintaining, developing and renewing of the functionality for and advice for, among others, the NVIS. Processor 2 delivers in this context including custom applications that have been specifically developed to facilitate the visa issuance process support.34 Processor 2 reports to the Director of Consular Affairs and Visa Policy of BZ.35

In Article 2.1 of the Processor Agreement (Appendix to the Agreement, Maintain and develop NVIS of 31 August 2010) states that with regard to the processing of

31 File 3, appendix 4b: Standard contractual clauses (processors).

32 File 3, appendix 4d: Appendix 1 to the standard contractual clauses

33 File 23, appendix 05: Organization chart Processor 2 worldwide for NVIS

34 File 14, appendix 02.1: GDPR Amendment Agreement Processor 2 – Min BZ NVIS 20180529, p.14.

35 File 14, appendix 02.1: GDPR Amendment Agreement Processor 2 – Min BZ NVIS 20180529, p. 1.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

36.

37.

38.

39.

personal data of BZ by Processor 2 under this Processor Agreement, BZ will

is the controller and that Processor 2 is the processor.36

It follows from Article 4.1 of the Processor Agreement between Processor 2 and BZ that Processor 2 sub-

can engage processors for the processing of personal data in the event of

prior written specific or general permission from BZ. Processor 2 must be based on the

agreement with BZ to impose the same obligations on sub-processors with regard to the

processing of personal data such as that to which Processor 2 itself is bound by this

Processing Agreement.

Article 5.1 of the processor agreement between BZ and Processor 2 establishes that BZ has the right to

has to have an audit by a certified internal or external auditor once per contract year

to Processor 2's compliance with its obligations under the processor agreement. the AP

has determined that BZ evaluates Processor 2's compliance by requiring so-called

assurance statements from Processor 2. The AP has received two assurance reports from BZ with

relating to Processor 2 for the period 1 November 2017 - 31 October 2018.37

The AP has established that Processor 2, in the context of its services for NVIS, has

company Processor 3 deploys as sub-processor. Processor 3 (formerly [CONFIDENTIAL]) develops and

operates data storage centers worldwide. In the Netherlands, Processor 3 has a data center in

Amsterdam. Processor 3 provides services to Processor 2.38, namely realizing the availability of

the data center, including physical facilities.

[CONFIDENTIAL]39

2.2.2 Legal assessment

Controller

In accordance with the VIS Regulation (Article 41(4)), each Member State for the processing of

personal data in the VIS to the authority to be considered as the controller responsible for the

central responsibility for data processing by this Member State. The responsible

has been notified to the European Commission and published in the Official Journal of the European

Union.40 On this basis, the Minister of Foreign Affairs has been designated as

36 File 14, appendix 02.1: GDPR Amendment Agreement Processor 2 – Min BZ NVIS 20180529.

37 File 14, appendix 12.2: [CONFIDENTIAL].

38 File 20: [CONFIDENTIAL].

39 File 20: [CONFIDENTIAL].

40 List of competent national authorities whose duly authorized staff have access to the Visa Information

System (VIS) to enter, modify, delete or consult data, OJ 2012, C79/05.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

40.

41.

42.

43.

44.

45.

46.

controller of NVIS. This is also confirmed by the Ministry to the AP

documents provided.41

The Minister (with the support of his ministry) determines how the visa applications

and also makes the final decision on visa applications. With that

the Minister determines the purpose and means for the processing of personal data within NVIS.

The AP establishes that the Minister of Foreign Affairs is the controller within the meaning of

Article 4, preamble under 7, GDPR, for the processing of personal data in the context of NVIS. In which

This decision is referred to as BZ, the AP equates this to the Minister of Foreign Affairs.

Processors

According to Article 43 of the Visa Code, Member States may cooperate with an external service provider who

data controller supports in the visa process. Member States are obliged to make agreements

make in a legal instrument where the minimum requirements are specified in the Visa Code.42

The AP notes that BZ engages a number of parties to process data in the visa process

namely Processor 1 (the third-party service provider handling the visa applications

takes), Processor 2 (for the application and technical management of NVIS) and Processor 3 acting as processor

provides support to the processes of Processor 2. There are with these parties

processing agreements. From the various processing agreements concluded between

these parties and BZ follows that the Minister is regarded as the controller and the

mentioned parties as processors.

The AP therefore establishes that Processor 2 and Processor 1 are processors as referred to in Article 4, under 8,

GDPR. Processor 3 is a processor engaged by Processor 2, as referred to in Article 28,

paragraphs 2 and 4 GDPR (sub-processor).

2.3 Security plan NVIS

2.3.1 Legal framework

Article 32(2) of the VIS Regulation requires each Member State to provide the necessary technical and organizational

establish security measures, including a security plan. This plan is one of the

security measures it must take to secure the data before and during transmission

to the NVS. Such an obligation also arises from Articles 32 and 24 GDPR. Article 24 GDPR writes

more generally ensure that the responsible measures in the area of compliance with the

GDPR and that they should be periodically reviewed.

Article 32(3) VIS Regulation further states that the managing authority must take the necessary measures

to achieve the objectives referred to in paragraph 2 with regard to the functioning of the VIS,

including the adoption of a security plan. The strategic principles and

41 For example, file 12, appendix 44a: pia application station signed and file 12, appendix 44b: nvis pia signed.

42 Appendix X Visa Code.

preconditions that BZ uses for information security in relation to NVIS must be clearly stated

the security plan. In concrete terms, this means that BZ must have drawn up a security plan

for the NVIS, in which at least attention is paid to points a to k included in Article 32, paragraph

2, VIS Regulation are included.

The Baseline Information Security Government (BIO) also writes the presence of a

information security plan that is periodically assessed, the following standards are relevant here:

47.

5.1.1

5.1.1.1

5.1.2.1

Information Security Policies

For information security, a set of policies should be

defined, approved by management, published and communicated to

employees and relevant external parties.

An information security policy has been drawn up by the organization. This policy is

established by the management of the organization and contains at least the following points:

a. The strategic principles and preconditions that the organization uses for

information security and in particular the embedding in and alignment with the general

security policy and the information provision policy.

b. The organization of the information security function, including responsibilities,

duties and powers.

c. The assignment of responsibilities for chains of information systems to

line managers.

d. The common reliability requirements and standards that apply to the organization of

are applicable.

e. The frequency with which the information security policy is reviewed.

f. Promoting security awareness.

The information security policy is periodically updated and in line with the (existing)

governance and P&C cycles and external developments reviewed and adjusted if necessary.

2.3.2 Actual findings

During the investigation, the AP asked BZ in writing questions about the security plan with

relating to personal data in NVIS. The AP also has the existence of a security plan and the

its contents checked in practice during the on-site investigation at the consular posts in

London and Dublin. Furthermore, the AP has requested written documentation relating to the

existence and content of a security plan.

Ministry of Foreign Affairs

The AP notes that, during the investigation, at the request of the AP43 to prepare a security plan (N)VIS

provided, replied with three documents, namely:

48.

49.

- Vulnerability analysis and IB plan DCV44

- PIA Request Station45

43 File 1: Announcement VIS investigation/ AP information request of 29 May 2019.

44 File 3, appendix 5a: Vulnerability analysis and DCV IS plan.

45 File 3, appendix 5b: PIA Application Station.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

- Quick scan Schengen visa February 201946

50.

51.

52.

53.

54.

The “Vulnerability Analysis and DCV Income Plan” of January 2015 contains a risk assessment, with regard to

to DCV's business processes for granting visas and the posts, which the DCV management has allowed

to comply with the obligations of the Information Security Regulation Decree
Rijksdienst 2007. The report contains, among other things, a report of the relevant threats and
vulnerabilities of the information systems. The report also contains measures that
reduce risks to an acceptable level. The report qualifies these proposed measures
as an 'information security plan' including prioritization.
The “PIA Request Station” concerns a Privacy Impact Assessment of the Request Station. It
end result of the PIA is a set of risks and recommendations for the security measures that
must be realized under the responsibility of DCV.
The “QuickScan Schengen visa February 2019” is a QuickScan that was carried out at the request of DCV to
the security requirements that are set from the business processes for the Schengen visa process where
special personal data are included. The purpose of the QuickScan is to be as objective as possible
determine the security requirements for the Schengen visa. This has also been looked at
whether these requirements fall within the Baseline information security or whether they rise above it. From the
QuickScan follows that the Schengen visa process falls outside the Baseline information security of BZ and that
additional risk analysis is required. This is instructed in the QuickScan.
Based on these three documents, the AP concludes that BZ has a number of different documents,
containing (intended) security measures. Some of those measures have
directly related to NVIS.
Consular Post London
During the on-site investigation on July 2, 2019 in London, the AP asked for completeness:
access to the security plan related to NVIS. The consular post in London has a
standard format security plan provided by the Ministry of Foreign Affairs and provided locally by the consular post
entered. Two inspectors from the AP and the FG of BZ have had access to the most recent version
of the security plan. [CONFIDENTIAL]:
[CONFIDENTIAL]
The documents mentioned relate to the security of the London consular post, in particular

[CONFIDENTIAL], and do not focus on the information security of NVIS and the visa process. the AP notes that she has seen documentation at the consular post in London that does not relate to the information security related to NVIS.47

46 File 3, appendix 5c: Quickscan Schengen visa February 2019.

47 File 8: Report of Official acts security plan OTP consular post London.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

55.

56.

57.

Consular Post Dublin

The AP also checked in Dublin whether there is in practice a security plan related to NVIS was available. During the on-site investigation on 22 January 2020 at the consular post in Dublin, stated that a security plan is in place. It concerns a standard format security plan that is BZ is delivered and filled in locally at the post. An adjustment of the security plan will be done once a year by the deputy chief of the post.48

On 23 January 2020, two inspectors from the AP and the DPO of the Ministry of Foreign Affairs, partly during the investigation, on site at the consular post in Dublin, upon request was given access to a security plan with regarding NVIS .49 [CONFIDENTIAL]:

[CONFIDENTIAL].50

The AP notes that documentation submitted at the consular post in Dublin does not refer to the information security related to NVIS.51

CSO The Hague

The AP has checked with CSO whether a security plan within the meaning of the VIS Regulation is available is. The AP notes that the CSO at the request of the AP52 to provide a security plan (N)VIS replied with 9 documents53, namely:

- Baseline information security BZ 2018, version 1.00 final;54
- Security Security Management Package, version 0.2 final;55
- Security plan Risk analysis reporting – [CONFIDENTIAL];56
- Security analysis of stolen secure mail CSO;57
- Security analysis burglary building;58
- Security analysis intrusion mer and ser;59
- Security example Unauthorized [CONFIDENTIAL];60
- Security example info in case of unexpected visit;61

48 File 27: Report of Official acts consular post Dublin.

49 File 28: Report of Official acts security plan OTP consular post Dublin.

50 On the spot, the AP inspectors established that access to this document was not necessary for the investigation.

51 File 27: Report of Official acts consular post Dublin.

52 File 13: AP information request of 25 July 2019.

53 File 14: BZ response of 8 August 2019 to AP Information of 25 July 2019.

54 File 14, appendix 14.1 Baseline information security BZ 2018 v1.00 Final.pdf.

55 File 14, appendix 16.1: Security Security Management Package 0.2 final.

56 File 14, appendix 16.2: Security plan Risk analysis report - [CONFIDENTIAL].

57 File 14, appendix 16.3: Security analysis of the theft of secure post CSO.

58 File 14, appendix 16.4: Security analysis building burglary.

59 File 14, appendix 16.5: Security analysis penetration mer and ser.

60 File 14, appendix 16.6: Security example Unauthorized persons [CONFIDENTIAL].

61 File 14, appendix 16.7: Security example info in the event of an unexpected visit.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

- Overview access CSO.62

58.

59.

These documents describe aspects of information security. The AP notes that these aspects

not specifically targeted or related to NVIS. There are also no concrete references to the

visa process found.

2.3.3 Legal Assessment

The AP has established that BZ has included certain security measures in various documents.

A number of these documents have been provided to the AP in response to requests for information

to the minister. Other documents have been brought forward at or following the visit of AP

to CSO.

60. The AP notes the following with regard to the documents submitted.

The “Vulnerability Analysis and DCV Income Plan” contains a number of security measures, but is not

current (dating from 2015). The local security measures, which were implemented during the on-site investigation

for the sake of completeness, have been inspected at the consular post in Dublin and London and the documents attached to

the

CSO have been requested, are not specifically aimed at NVIS and only concern a limited number

security measures (and not on information security) that pursuant to Article 32 VIS Regulation

are prescribed. The measures in these documents mainly relate to the broad security of

buildings and systems, including related potential security risks. The AP notes that

an overarching security plan with regard to NVIS, with attention to the measures, such as

laid down in Article 32, paragraph 2, under a to k of the VIS Regulation, is not present.

In its view, BZ states that the AVG, the VIS Regulation and the BIR/BIO do not impose any requirements on the form of a security plan nor does it require a security plan that is solely on the national visa information system. BZ considers a number of documents together as a security plan for NVIS63:

- Privacy Impact Assessment Schengen and Caribbean Visa of 25 October 2018.
- Baseline test NVIS
- Quick scan Schengen visa February 2019 and the Risk analysis 'Vulnerability analysis and IB plan' DCV'.

In its opinion, BZ has indicated that BZ has regretted that it has information request from the AP the first two documents have not been provided to the AP. BZ further notes that the external auditor who, on behalf of the AP, has judged in the context of the VIS audit that BZ the Baseline test, PIA and the risk analysis meet the standard that a security plan has been established.

The AP does not follow BZ's view. At various times during the investigation, the AP asked about the NVIS security plan. BZ had several options to obtain the relevant documents provide. The AP sees this ex officio investigation and the VIS audit carried out by the external party performed as two separate trajectories that did not take place at the same time. The VIS audit was

61.

62.

63.

62 File 14, appendix 16.8: Overview access to CSO.

63 Written Opinion BZ of 15 October 2021, p. 4.

64.

65.

66.

67.

broader in scope and used a different assessment framework. In addition, the external auditor only established that 1) not he but BZ the combination of the Baseline test, PIA and risk analysis together regarded as an Information Security Plan and 2) a concrete information security plan around the Visa process is missing.

The AP has assessed the newly submitted documentation from BZ. The AP notes that the 'Privacy' Impact Assessment Schengen and Caribbean Visa of 25 October 2018', as the title suggests, a Privacy Impact Assessment concerns. This is a very useful tool to mitigate the privacy risks of a data processing, but does not form a plan that focuses on information security in are whole. The submitted 'Baseline test NVIS' is a kind of completed questionnaire/checklist. It is a list of BIO standards with assignments for making and taking security measures, where it is not understandable for the AP how the given answers should be be interpreted. Based on these documents, it is unclear to the AP which policy measures and BZ has concretely taken control measures for NVIS.

The form of a security plan is free, but the strategic principles and preconditions that BZ uses for information security in relation to NVIS must be clear from the security plan to turn out. In addition, Article 32(2) of the VIS Regulation requires BZ to have a security plan drawn up for NVIS, in which at least attention is paid to points a to k of article 32(2) VIS Regulation. In the opinion of the AP, BZ has not sufficiently demonstrated this. BZ has for example, did not submit a security plan stating which preconditions apply to the physical security of NVIS that guarantees the appropriate protection of personal data is becoming. Nor has the AP received a formal procedure from BZ that describes how and when BZ performs checks on logging. The general procedure that BZ has at the time of the investigation

provided for reporting security incidents by BZ employees, was not satisfactory. And the
procedures about granting and checking access rights to the NVIS environment have only been implemented by BZ
established in January 2022. The AP refers to sections 2.4, 2.5, 2.6 and 2.7 for the comprehensive review
of these procedures. The AP concludes that the documents presented by BZ as - in their entirety
viewed - an information security plan does not meet the preconditions to be set for it.
In view of the BIO standards, the AP further notes that due to the lack of (essential parts in)
information security policy, this policy not at scheduled intervals (or if significant
changes occur) has been assessed by BZ to ensure that it is continuously appropriate, adequate
and effective. Securing information is a process in which a Plan-Do-Check-Act is always
cycle must be completed, as laid down in, among other things, BIO standard 5.1.2.1.
In its opinion, BZ has provided a number of documents about the PDCA cycle it has gone through.64
The AP has established in this regard that BZ is at a high level in the 'Baseline information security BZ 2021'
abstraction level has determined who is responsible for the implementation and execution of BIO standards
is responsible. The Personal Data Protection Policy describes the PDCA cycle at
with regard to the protection of personal data, but does not contain the security aspects thereof.
The same applies to the document Grip on privacy, the GDPR manual, in control statements and the
submitted follow-up memo. With risk analyzes from 2015 and 2020 and a plan of measures, BZ has
64 Written Opinion BZ of 15 October 2021, p. 4.

68.

69.

November 2021 show that it only occasionally has security measures in place with regard to NVIS

evaluated and acted upon.

Based on the above, the AP comes to the conclusion that BZ does not have a security plan (and this has also not evaluated) that meets the requirements of Articles 24 and 32(1) of the GDPR and further detailed in Article 32, paragraph 2, preamble, VIS Regulation and BIO standards 5.1.1, 5.1.1.1 and 5.1.2.1.

2.4 Physical security access to NVIS

2.4.1 Legal framework

Article 32(2)(a) of the VIS Regulation requires measures to be adopted to:

physically protect data, including preparing contingency plans for the physical infrastructure. This requirement is also laid down in general terms in Article 32 GDPR. Furthermore, in the BIO standards included that illustrate where physical security can be controlled become. The BIO does not literally describe goals to be achieved (the “what”) must be arranged. The AP has checked the physical security on the basis of a checklist (see explanation in the next section). The following provisions from the BIO are for the assessment of this checklist relevant:

11.1.1

11.1.2

11.1.3

11.1.4

11.1.5

11.2.2

Physical Security Zone

Security zones should be defined and used to define areas protect those sensitive or essential information and information processing facilities contain.

Physical access security

Secure areas should be protected by appropriate access security to prevent

ensure that only authorized personnel have access.

Securing offices, spaces and facilities

Physical security should be designed for offices, spaces and facilities and

applied.

Protect against outside threats

Physical protection against natural disasters, malicious attacks or accidents should be

to be designed and applied.

Working in secure areas

Procedures should be developed for working in secure areas and

applied.

Utilities

Equipment should be protected from power outages and other disturbances that

caused by disruptions in utilities.

2.4.2 Factual Findings

The AP has examined the physical security at the consular posts in London and Dublin, the CSO in Den

Haag, Processor 2 in Utrecht and Processor 3 in Amsterdam. During the checks, the AP has per location

70.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

71.

72.

used two (identical) checklists. The first checklist focused on physical security

of the building and the second checklist on the physical security of the areas in which access to the

NVIS environment is possible and/or the intake process for Schengen visas takes place.65 Below is per location describes the situation found during the on-site investigations.

Consular Post London

[CONFIDENTIAL]66

Processor 1 London

[CONFIDENTIAL] 67

65 [CONFIDENTIAL]

66 File 7: Report of Official Operations OTP Consular Post London.

67 File 9: Report of Official Acts OTP Processor 1 London.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

73.

74.

Consular Post Dublin

[CONFIDENTIAL] 68

CSO The Hague

[CONFIDENTIAL]69

68 File 27: Report of Official Acts OTP consular post Dublin.

69 File 11: Report of Official Acts OTP CSO 18 July 2019 and 12 September 2019.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

75.

76.

77.

Processor 2 Utrecht

[CONFIDENTIAL]

Processor 3 Amsterdam

[CONFIDENTIAL]70 71 72

2.4.3 Legal Assessment

First of all, the AP establishes that measures have been taken at all locations investigated in the field of physical security. The AP concludes that measures have been taken to protect the buildings and space(s) in which data of visa applicants are processed physically, including with cameras and motion sensors. Furthermore, the AP concludes that the spaces in which personal data of visa applicants are treated as secured areas.

70 File 19: Report of Official Acts OTP Processor 3 November 8, 2019.

71 File 20: [CONFIDENTIAL]

72 File 21: Email BZ of 13 November 2019 with documents related to OTP 8 November.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

78.

79.

80.

81.

82.

However, the AP notes that the Ministry of Foreign Affairs has not explicitly determined which parts of the IT infrastructure should be regarded as the critical infrastructure of the visa process. In this case to be able to comply with Article 32 GDPR jo. 32(2)(a) of the VIS Regulation, this is a requirement. BZ has stated in its view that it has criticized several systems in the spring of 2020 determine. During the opinion session on 4 November 2021, the Ministry of Foreign Affairs submitted an (undated) list of information systems to the AP, after which BZ indicated which systems were considered critical infrastructure have been identified. NVIS is one of those systems on this list and has therefore been approved by BZ classified as critical infrastructure.

The AP also found during on-site investigations that BZ has no emergency plans designed to protect the physical infrastructure of the visa process. The Consular Post in London, the consular post Dublin and CSO do not have an emergency power supply while paragraph 11.2.2 of the BIO stipulates that equipment should be protected against power failure. This means that BZ, when it comes to contingency planning and protection of equipment against disruptions in utilities, in the opinion of the DPA does not comply with the provisions of Article 32(1) of the GDPR and further elaborated in article 32, paragraph 2, sub a, VIS Regulation and organic standards 11.1.4 and 11.2.2.

In its opinion, BZ has indicated that BZ has concluded from its own threat analyzes that flood detectors and emergency power supplies at London and Dublin stations are not required.

The AP partially agrees with this view. Flood detectors can be dispensed with after a explicit risk assessment. Regarding power outages, BIO requires that equipment should be protected against power outages and other disturbances caused by disruptions in utilities. Critical infrastructure such as NVIS must be highly secured, with the business interruption should be avoided as much as possible. BZ has insufficient explained why NVIS as a critical system does not need an emergency power supply.

Furthermore, the AP notes that with regard to the spaces at the consulate in London, where work has been done with visa stickers and the NVIS system, there were shortcomings in terms of physical

security. [CONFIDENTIAL]. Now that in practice there were no security guarantees when entering of the zone that must be extra secured, the AP determines that the physical security of the rooms in which work on the visa process in London did not comply with Article 32(1) GDPR and further elaborated in Article 32, paragraph 2, sub a, VIS Regulation and BIO standards 11.1.1 to 11.1.5 and 11.2.2. In its opinion, BZ has stated (and submitted supporting documents) that it appears that in the past two years of measures have been taken to secure access to the consular section.73 [CONFIDENTIAL]. The AP notes that the shortcomings in the field of physical security in the consulate in London have since been remedied.

73 Written Opinion BZ of 15 October 2021, p. 5.

83.

84.

85.

86.

The AP has further established that with regard to the activities of Processor 2 in the context of the visa process, it is important that Processor 2 employees are predominantly place and time independent allowed to work. As soon as work is done outside the buildings of Processor 2, the physical security guarantees at the locations of Processor 2 obviously do not help. The legal requirement that personal data of visa applicants may only be processed in areas with adequate physical however, security remains unaffected. It is unclear to the AP how data within databases of NVIS are physically protected in case of location and time-independent work by employees of Processor 2 who are stationed in both the Netherlands and [CONFIDENTIAL]. The AP has during the

investigation did not receive any documentation from BZ regarding the physical protection of NVIS data at work independently of place and time. As the data controller, BZ must ensure appropriate security measures for the physical protection of NVIS data, and the verify the effectiveness of these security measures.

In its view, BZ states that there are sufficient security guarantees for employees of Processor 2 working from home. First of all, unauthorized persons do not know where Processor 2 employees live and immediately disconnects from the network and management VPN if a laptop from a house is stolen. Setting up the VPN connection works through multi-factor authentication and there is a strict employee policy. BZ has issued two regulations in that regard.74

The AP has assessed these regulations and as far as place and time-independent working are concerned, it stands states that the employee must take all necessary precautions when using the personal device in a public place so that the screen cannot be viewed by others.

It is not clear, however, which precautions are expected from an employee. In reaction to this, the AP asked BZ whether and under what conditions employees of Processor 2 are allowed to work with NVIS in public places, how BZ assesses Processor 2's work-from-home policy and which written agreements between BZ and Processor 2 about the physical security of NVIS at places and time-independent work there are. Finally, the AP has requested a number of audit statements.

BZ has stated that all employees of Processor 2 involved in the NVIS services have the apply office policy for remote working, which in theory can also take place outside one's own home

75 BZ has assessed Processor 2's homeworking policy as sufficient on the basis of the already previously issued employee policies. However, the AP notes that in the submitted by BZ control statements, audit statements and the processing agreement the subject of place and time working independently has not been treated/assessed.76 It is therefore unclear to the AP on the basis of which considerations BZ has judged to be sufficient for working independently of place and time.

74 Written Opinion BZ dated 15 October 2021, appendices 19 and 20.

75 E-mail BZ of 10 December 2021.

76 E-mail BZ of 10 December 2021, appendix 11.1 to 13.3.

[CONFIDENTIAL]

87.

88.

89.

90.

91.

Based on the above, the AP is of the opinion that BZ has not demonstrated that there is sufficient safeguards apply to physical security when working in NVIS in public places. As indicated in section 2.1.2 BZ processes a great deal of - including - special personal data in NVIS. This makes the nature of the processing is sensitive and the negative consequences for data subjects in unlawful processing can be significant. In addition, BZ uses the NVIS system as a critical infrastructure designated. While there is a pass access system and camera surveillance at the consular posts and CSO is applied, such safeguards are not present in public areas.

Since BZ has not demonstrated that there are sufficient guarantees for physical security at the working in NVIS in public spaces and BZ also does not have the effectiveness of the policy in this regard checked, the DPA concludes that there has been an infringement of Article 32(1) of the GDPR and further elaborated in Article 32, paragraph 2, under a and k of the VIS Regulation.

2.5 Access rights to NVIS and personnel profiles

2.5.1 Legal framework

Article 6(1) VIS Regulation provides that only duly authorized staff of the visa authorities have access to the VIS for the purpose of entering, modifying or deleting

visa details. Article 32(2)(f) of the VIS Regulation requires that the necessary measures are established to ensure that those authorized to consult the VIS only have access have access to the data to which their access authorization relates and only with personal and unique user identities (data access control).

Article 32(2)(g) of the VIS Regulation requires that the necessary measures be adopted to: to ensure that all authorities with a right of access to the VIS create profiles in which the tasks and responsibilities are described of the persons authorized to access data, on access, update, delete, and search these profiles, upon request and without undue delay to be made available to the national supervisory authorities, as referred to in Article 41 (staff profiles). This is also described in Article 28(4)(c) of the VIS Regulation which states that “each Member State is responsible for the management and arrangements under which appropriately authorized staff of the competent national authorities in accordance with this Regulation access to the VIS, and the establishment and regular updating of a list of such staff members and their profiles”.

Article 32(2)(k) VIS Regulation requires that the necessary measures be adopted to: verify the effectiveness of the security measures referred to in this paragraph and with regard to internal control to take the necessary organizational measures to ensure that these regulation is complied with (internal control). This is in line with the generally determined in Article 32 of the GDPR.

The BIO is obliged to allocate management and implementation measures internally. From the information security policy must show which roles within an organization are responsible for

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

the measures to be taken. It is important that security procedures by the relevant

responsible are determined. The following provisions of the BIO are specifically relevant:

9.2.1

9.2.2

9.2.5

9.2.6

User Registration and Logout

A formal registration and deregistration procedure should be implemented to

to allow the allocation of access rights.

Grant users access

A formal user access grant procedure should be implemented

to grant access rights for all types of users and for all systems and services

to reject or withdraw.

Assessment of user access rights

Asset owners should regularly review user access rights

judge.

Revoke or modify access rights

The access rights of all employees and external users for information and

information processing facilities belong to the termination of their employment,

contract or agreement should be removed, and changes should be made

amended.

2.5.2 Actual findings

During the investigations, the AP asked BZ questions about the organization of access rights to

NVIS and its internal control. For this, the AP has the current authorization lists,

personnel profiles, authorization procedures and other relevant documentation requested regarding

to granting access rights to the NVIS environment. The AP's investigation focused on the

following questions regarding access rights:

- Does BZ have established procedures for granting and controlling access rights

to NVIS?

- Has drawn up BZ personnel profiles with regard to NVIS in which the tasks and

responsibilities are described of the persons authorized to process data in the

access, record, update, delete and search the system? Are NVIS

personnel profiles updated regularly?

- Are the assigned access rights (authorization lists) regularly assessed?

The AP has only investigated this part of the parties that have access to the NVIS environment.

92.

93.

2.5.2.1 Procedures on granting and controlling access rights to NVIS

Consular Post London

BZ has provided the AP with three documents relating to authorization procedures in connection

with NVIS: (1) 'NVIS Data Management Manual'77, (2) a document entitled 'Authorization procedure

NVIS Embassy London'78 and (3)'Work instruction/procedure: logging authorizations applications'.79

The first document is in the form of a practical user manual, where it is not clear

which responsible person within BZ has established this manual. In chapter 3 of the document

contains a short paragraph on granting access rights to NVIS, stating all

practical steps in the system regarding the assignment and removal of NVIS roles and

the change of the authorization period. It is further stated that the management of the tasks at the NVIS

roles in the department by the Consular Affairs and Visa Policy Department, cluster Information Management and Management (hereinafter: DCM/MB-IB) is performed. 80 The document shows not with whom the responsibility has been placed for assigning, changing and controlling authorizations.

The second document is one page, undated and not (at a management level) established. It has not become clear to the AP whether this document was drawn up in response to its request for information, or whether it existed before. The document describes how employees of the consular post in London gain access to NVIS.81 It also states document: “in addition to the annual check by functional management, ad hoc checks (of the authorisations) in the post.”.

The third document consists of two pages and concerns the verification of authorizations. It says in it stated the following: “For the purpose of checking logging authorizations, DCV/MB-IB requests the items and RSOs once a year (after the annual transfer round) to check which employees who should have roles in certain applications...”. The document also contains flowcharts schematically depicting a 'check on logging authorizations applications'. It document is generically and non-specifically aimed at controlling access rights to NVIS. The piece is undated and has not been established (at a management level).

Based on the check at the consular post in London, the AP finds that BZ is not about formally has established procedures for granting, changing and terminating access rights to

94.

95.

96.

97.

98.

77 File 3, appendix 1: NVIS Data Management Manual February 2018.

78 File 12, appendix 04: Authorization procedure NVIS Consular post London.

79 File 3, appendix 6b: Work instruction logging and authorization applications.

80 File 3, appendix 1: NVIS Data Management Manual February 2018, p. <16: “..NVIS automatically takes over all employee names

off [CONFIDENTIAL]. ICT manages this technical functionality. Therefore, no employees can be added manually in NVIS. An employee can only access NVIS if he or she is authorized for a certain role. Roles determine what an employee can and cannot do

do within NVIS. A role consists of several tasks. Each task provides access to a specific NVIS component. Managing the tasks at the

rolling is performed in the department by [CONFIDENTIAL].”

81 File 3, appendix 1: NVIS Data Management Manual February 2018: “Access to NVIS is linked to the BZ account of the employee and the post where this employee works. When the employee leaves the post, access to NVIS is automatically disabled

terminated because the employee's BZ account at the post is closed or transferred to another post. [CONFIDENTIAL]

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

NVIS. Nor does BZ have established procedures to limit the access rights granted to NVIS

to check.

Consular Post Dublin

Prior to the investigation in Dublin82, the AP BZ requested in writing83 to

authorization procedures NVIS and other relevant documentation related to the establishment of

access rights to NVIS. BZ has published a document entitled 'NVIS Embassy Authorization Procedure'

Dublin'84 provided to the AP.

99.

100. The document consists of half a page of text, is undated and is not at (management level) established. It has not become clear to the AP whether this document was drawn up in response to its request for information, or whether it existed before. The document submitted describes that the supervisor will be granted an application with [CONFIDENTIAL]. Access to NVIS is linked to [CONFIDENTIAL]. The [CONFIDENTIAL] controls changes to the NVIS accounts and roll. Furthermore, the annual control of the granted authorizations by [CONFIDENTIAL] executed.

102.

101. Following its investigation at the Dublin consular post, the AP establishes that BZ does not have formal procedures for granting, changing and terminating access rights to NVIS and for checking the authorizations granted to NVIS.

CSO The Hague

During the investigation of the AP, the interviewed CSO employees provided an explanation about the procedure followed by the CSO when obtaining access rights to NVIS.85

[CONFIDENTIAL]

When granting access rights to NVIS, the CSO uses the 'Manual Data management NVIS'86 (the description of this document can be found in section 2.5.2). Also does the CSO have work instructions87 [CONFIDENTIAL]. The (undated) work instruction exists from 13 unnumbered pages. It is unknown whether the document has been adopted at the management level. It is not clear from the document who is formally responsible for granting authorisations, the implementing changes in the accounts, assigning NVIS roles and checking this. the AP concludes as a result of its investigation at the CSO that it has not been found that BZ has

103.

82 File 27: Report of Official Acts OTP consular post Dublin.

83 File 25: Announcement OTP consulate Dublin and AP information request of 19 December 2019.

84 File 26, appendix 4.1: Employee - Roles – Dublin.

85 File 11: Report of Official Acts OTP CSO 18 July 2019 and 12 September 2019.

86 File 3, appendix 1: NVIS Data Management Manual February 2018.

87 File 14, appendix 23.1: Assigning work instructions NVIS roles at CSO.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

formal procedures regarding granting, changing and terminating access rights and the control of the granted access rights to NVIS.

Processor 2

104. As a result of the investigation88 that the AP conducted at Processor 2, the following are: documents related to authorizations provided: (1) an internal access procedure management system,89 (2-4) authorization procedure of Cloud Infrastructure Management, consisting of three documents90, and an authorization list91 with names of Processor 2 employees who have access authority to the NVIS platform and databases.

105. The submitted authorization procedures (1 to 4) describe the working method that is used at Processor 2 applied when creating, changing and/or deleting employee accounts. Further contain the procedures schematic representations of the (practical) steps that are relevant for the application, change and remove access rights to the systems Processor 2 works with. In addition the authorization procedures deal with the types of accounts that employees can have. Through a further explanation by the Ministry of Foreign Affairs during the opinion phase, it has become sufficiently clear to the AP what the relationship is between these types of accounts and responsibilities on the one hand and the NVIS environment on the other.92

2.5.2.2 Personnel profiles

Consular Post London, Consular Post Dublin and CSO

106. BZ has provided a generic document entitled 'NVIS profiles'.93 It is a table in which the know NVIS roles are related to tasks that fall under the assigned NVIS role. The tasks are briefly indicated and it is unclear with which concrete actions (e.g. viewing data, record, update, delete and search) in the NVIS context. Furthermore, the relationship between the position of the employee and the assigned NVIS roles and tasks not described.

107. The AP has requested BZ to provide personnel profiles94 relating to the employees of the CSO. BZ has submitted a text95 template with result areas and competencies, which may be used for the description of vacancies at the CSO. The description included in this document does not cover the duties and responsibilities in relation to actions in NVIS.

108. During the investigation, the AP established that BZ did not draw up personnel profiles in which the tasks and responsibilities are described of the staff at the consular post in London,

88 File 17: Report of Official Acts OTP Processor 2 1 November 2019.

89 File 17, Appendix 8: [CONFIDENTIAL].

90 File 18, Appendix 3: [CONFIDENTIAL]; File 63: [CONFIDENTIAL]; and File 18, Appendix 1: [CONFIDENTIAL].

91 File 21, appendix 4: Authorization list NVIS.

92 BZ opinion 14 October 2021, p. 8 and letter from the Ministry of Foreign Affairs to AP dated 19 November 2021, appendix 1 Interview report, p. 33 and 34.

93 File 5, appendix 1: NVIS profiles.

94 File 4: AP information request of 13 June 2019.

95 File 16, appendix 2.1: Job profiles CSO visa, version 15 October 2019.

[CONFIDENTIAL]

consular post Dublin and CSO authorized to access, update, delete and . data in NVIS

to search.

2.5.2.3 Control of access rights to NVIS

Consular Post London

109. BZ has an up-to-date authorization list96 of all employees of the consular post in London to the AP

110.

submitted.

At the time of the investigation, 17 employees of the London consular post were working with the

access rights to NVIS. The following (several) NVIS roles have been assigned to these employees:

[CONFIDENTIAL].

Most employees had more than two NVIS roles, with a maximum of six NVIS roles

owned by one employee.

111. The AP has further checked the [CONFIDENTIAL] role. On the authorization list that BZ has given to the AP

provided was one employee (hereinafter: employee X) listed with this NVIS role. [CONFIDENTIAL].

Employee X had not worked at the Consular department for a long time, but did as

[CONFIDENTIAL] at another department of the embassy. For current work,

employee X does not need access to NVIS. During the AP check it turned out that logging into the

system in the role of [CONFIDENTIAL] was still possible. After logging in, employee X

view and change current NVIS data.

112. The authorization list provided also shows that some staff of the London consular post

113.

possessed an authorization with mutually incompatible NVIS roles,97 such as that of

[CONFIDENTIAL]. No motivation was included in NVIS in which the granting of this

conflicting roles was explained.

At the time of the investigation at the consular post in London, BZ also stated that the NVIS

granted authorizations once a year are checked by [CONFIDENTIAL]. At the consular post London is [CONFIDENTIAL] responsible for reporting all changes in the NVIS access rights.98 The operations manager was not present during the investigation and it is unknown how often the changes related to NVIS access rights to [CONFIDENTIAL] become passed. BZ has not provided any documents99 showing when the last check of the authorizations and NVIS roles at the London consular post.

114. The AP establishes that at the time of its check at the consular post in London, an employee wrongly had access rights to NVIS. At the time of the AP investigation, this employee was appointed to another position at the embassy, which did not require the use of NVIS. Further several employees of the consular post in London had NVIS roles that are incompatible. During the investigation, the AP did not provide any justification for the incompatible roles in NVIS found and received documentation showing when the last check of the authorizations and NVIS roles has taken place.

96 File 3, appendix 7: Overview of NVIS authorizations ZMA London.

97 The mutually incompatible NVIS roles are listed in File 12, Appendix 06a: Tasks - roles - incompatible - NVIS.

98 File 7: Report of Official Operations Consular Post London.

99 File 10: AP information request of 12 July 2019.

Consular Post Dublin

BZ has submitted an overview of the authorizations granted at the consular post Dublin to the AP.100 At the time of the investigation there were six employees working at the consular post who were had access rights to NVIS, in the following assigned NVIS roles:

[CONFIDENTIAL].

Two employees held NVIS [CONFIDENTIAL] roles that are mutually incompatible.

The assignment of these conflicting roles in NVIS was at the time of the investigation by or on behalf of BZ not further motivated.

During the investigation of the AP, the staff of the Dublin consular post stated that one the list of all granted authorizations is checked at the consular post once a year. In addition the Functional Management department in The Hague carries out checks on the granted authorizations.101

CSO

115.

116.

117. During the investigation, the CSO stated that the assigned NVIS roles focus on the segregation of duties. The roles of registration and decision are mutually incompatible according to the functional design of the NVIS application.102

[CONFIDENTIAL]103

The AP found no motivation in NVIS with regard to [CONFIDENTIAL].

118. The overview provided to the AP 'NVIS role division per function'104 shows that the CSO 79 employees have access to NVIS. The list includes the following functions:

[CONFIDENTIAL].

Three or more NVIS roles are assigned to these functions. Regarding the role [CONFIDENTIAL] it appears from the investigation of the AP that these rolls have not been in use for several years.105

119. The above overview also shows that some NVIS roles, over which some employees of the CSO are regarded as mutually incompatible.106 This concerns the following NVIS Roles: [CONFIDENTIAL].

100 File 26, Annex 4.1: Employee - Roles – Dublin.

101 File 27: Report of Official Acts OTP consular post Dublin.

102 File 11: Report of Official Acts OTP CSO 18 July 2019 and 12 September 2019.

103 File 16, appendix 3.1: Process Description Registration Department, version 1 August 2019.

104 File 14, appendix 23.2: NVIS division of roles per function.

105 File 5, Annexes 2 and 3 and File 11.

106 File 14, appendix 23.2: NVIS division of roles per function.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

120.

During the investigation, the CSO did not submit any documents to the AP that could explain the substantive motivation about the conflicting NVIS roles.

During the investigation on July 18, 2019, the CSO stated that the control of the attribution of authorizations are carried out in accordance with an internal control plan. The granted authorizations are changed twice a year year by [CONFIDENTIAL]. In addition, an inspection is carried out once a year by [CONFIDENTIAL].

[CONFIDENTIAL]107

The CSO also submitted the management report April 2018108 to the AP on 8 August 2019, showing that the authorizations granted to NVIS, including the NVIS roles, have been checked. The last audit took place in 2018.

121. The AP notes that the authorizations granted for access to NVIS are checked at the CSO.

122.

123.

The AP also establishes that several employees at the CSO have been awarded mutually incompatible NVIS roles, and that [CONFIDENTIAL] employees over have access rights with [CONFIDENTIAL] in NVIS. The motivation of the mutual

incompatible roles is missing in NVIS. Finally, some CSO employees had a role that was not

was more in use.

Processor 2

At the time of the investigation, the AP concluded that BZ did not provide any documentation

showing (sufficiently) which agreements have been made with Processor 2 about the procedures with regard to

of access rights between the controller and processor.

In its view, BZ states that the agreements between it and Processor 2 regarding access rights to NVIS

follow from agreements between BZ and Processor 2. BZ also has a quarterly report in that regard

about the control of these access rights of Processor 2.109 The AP has submitted these documents

assessed and concludes that no violation of Article 32(2) can be established on this point,

under k, VIS Regulation and will therefore not discuss this further in the legal assessment below.

2.5.3 Legal Assessment

Consular posts London and Dublin and CSO

124. As a result of its investigation, the AP finds that the consular posts in London and Dublin and the

CSO have access to NVIS.

[CONFIDENTIAL]

107 File 14: BZ's response of 8 August 2019 to the AP information request of 25 July 2019. Written answer to the question

from the AP: 'Who is

formally responsible for monitoring NVIS use at the Ministry of Foreign Affairs and specifically at the CSO?'

108 File 14, appendix 24.1: Visa management report April 2018, version 30 May 2018.

109 Written Opinion BZ of 15 October 2021, p. 8.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

125.

126.

Procedures about granting and checking access rights to NVIS environment

When allocating access rights, including NVIS roles, BZ uses the method used in

the practice is almost identical for the employees of the examined consular posts and the CSO in

The Hague. The AP notes that BZ does not have formal registration and deregistration procedures at its disposal

regarding the allocation of access rights to NVIS to employees. The AP considers that there are

although use is made of a manual to the system,110 in which all kinds of practical

steps have been explained, but that this is an unofficial user access grant procedure

includes with regard to registering and deregistering authorizations. The other documents111 that are as

authorization procedures issued by BZ concern an undated, summary description of the

method that BZ uses when authorizing employees of the consular posts and are not

formally established registration and deregistration procedures. The AP has established that that BZ is in conflict on this point

acts in accordance with Article 32(1) of the GDPR and further elaborated in BIO standards 9.2.1 and 9.2.2.

In its opinion, BZ has indicated that the existing work instructions will be formally implemented by 1 January 2022 at the latest

be determined.112 The AP received that document on January 9, 2022, and is of the opinion that it contains

the procedure for applying for, changing and stopping access rights in NVIS is sufficient

described.113

Personnel profiles

127. During the investigation, the AP established that BZ did not draw up personnel profiles in which the

128.

tasks and responsibilities are described of the staff of the consular posts

London and Dublin authorized to access, record, update, delete data in NVIS

and search. With regard to the personnel profiles114 of the employees at the CSO, it is

the AP is of the opinion that these profiles provide insufficient insight into the tasks and responsibilities of

the CSO employees who are authorized to process data in NVIS.

In its view, BZ states that the access rights allocated to the functions are determined on the basis of

of tasks and responsibilities.115 As a result of this, the AP again has documentation

asked what this should be. BZ has provided an authorization matrix dated January 7, 2014.116

Based on this, the AP comes to the conclusion that BZ does have personnel profiles that are sufficient

provide insight into the tasks and responsibilities of authorized employees. It follows that

In the opinion of the AP, BZ has acted in accordance with Article 32(2)() on this point

g, VIS Regulation. This provision also prescribes that personnel profiles must be available and

must be provided at the request of the AP.117 The AP must conclude that this BZ at the time of

the investigation by AP has not provided the complete personnel profiles, at the time the AP

requested it. It follows that BZ has acted contrary to Article 32(2)(g) on that point.

FISH Regulation.

110 File 3, appendix 1 and File 26, appendix 1.1: NVIS Data Management Manual February 2018.

111 File 12, appendix 4: Authorization procedure NVIS consular post London; and File 26, Annex 3.1: NVIS authorization

procedure

consular post Dublin.

112 Written Opinion BZ of 15 October 2021, p. 6.

113 E-mail BZ to the AP of 9 January 2022, BZ process NVIS authorization.

114 File 16, appendix 2.1: Job profiles CSO visa.

115 Written Opinion BZ of 15 October 2021, p. 7.

116 E-mail BZ of 10 December 2021, annex 14.

117 In view of Article 41(1) of the VIS Regulation, the AP is the competent supervisory authority

Control access rights to NVIS

129. First of all, the AP established that BZ does not have formal procedures with regard to the periodically checking the granted access rights to NVIS and NVIS roles. From the by BZ the documentation provided118 shows that the authorizations granted once a year by [CONFIDENTIAL] are checked. In addition, it has been stated that internal checks are carried out at the consular office posts in London and Dublin and at the CSO.119

130. The AP considers that it did not receive any documents during the investigation from which the frequency

131.

132.

133.

evidenced by the checks by [CONFIDENTIAL]. Nor has BZ demonstrated when the most recent control has been performed. With regard to the internal controls, the AP considers that in the event of the consular post London no documents have been provided that relate to the internal controls of the assigned authorizations. With regard to the CSO and the Dublin consular post, the AP establishes on the basis of the information provided120 that some internal controls related to past authorizations have occurred. The last internal audit at the CSO took place in April 2018. The consular post Dublin carries out checks at least once a year; the last check was done in 2019.121 Furthermore, the AP has established that several employees of CSO and an employee of the consular post London had NVIS role(s) that they did not need and some roles were found to be had not been in use for some time. This indicates that the granted access rights to NVIS and NVIS roles have been insufficiently checked.

During the opinion session, BZ stated that [CONFIDENTIAL] at consular posts are responsible for controlling access rights to NVIS. The one-off autumn check of [CONFIDENTIAL] acts as a safety net.122 BZ has further indicated the procedure for checking formally establish access rights.

In response to this, the AP requested documentation from BZ of the checks that [CONFIDENTIAL]

of the consular posts in London and Dublin on access rights to NVIS from 2018 to

with 2021. BZ has provided the following in response to this: authorization lists (from 2019, 2020 and 2021),

the withdrawal of access rights of one employee in 2019 and two evaluation reports that are no longer

then give a general picture of the screening of consular posts (from 2018 and 2019). The by BZ

The documents submitted do not lead the AP to a different opinion. The AP establishes that BZ has not

demonstrated that the operational managers of the London and Dublin consular posts regularly check

performed on the access rights to NVIS.

118 File 3, appendix 1: NVIS Data Management Manual February 2018; File 12, Annex 4: Authorization procedure NVIS

Consular post

London; and File 26, appendix 3.1: Authorization procedure NVIS consular post Dublin.

119 File 7: Report of Official Operations Consular Post London; File 27: Report of Official Operations Consular Post Dublin;

and File 11: Report of Official Acts CSO 18 July 2019 and 12 September 2019.

120 File 14, appendices 24.1 and 24.2: Visa Management Report Apr 2018 and Visa Management Report Sep 2018; and File

27, appendix

6: 6. Correspondence about adjusting NVIS roles.

121 File 27: Report of Official Acts OTP Consulate Dublin.

122 Letter from the Ministry of Foreign Affairs to AP dated 19 November 2021, appendix 1 Interview report, p. 30.

134. With regard to the procedure provided by BZ on the control of access rights, the DPA notes

that this describes the process surrounding the one-off autumn audit of [CONFIDENTIAL].123 The

AP has established that in these proceedings no clarity is provided about how BZ ensures

that access rights are checked regularly. The one-off autumn check functions, like BZ

sets, as a safety net. Given the type of data processing in NVIS, the DPA considers an annual check insufficient to ensure that only authorized employees have access to this system. This one working method does not sufficiently mitigate the risk that an employee who changes position will falsely accessing NVIS, [CONFIDENTIAL].

135. The AP has also established that an employee at the consular post in London wrongly had access rights to NVIS in the role of [CONFIDENTIAL], and this allowed NVIS data to view and mutate. This employee was appointed to a different position at the embassy, for which the use of NVIS was not necessary. In its opinion, BZ has stated that the [CONFIDENTIAL]-application was deficient at the time of the investigation, as a result of which the [CONFIDENTIAL] role was still should be kept in case the [CONFIDENTIAL] application would not function. This argument fails. An employee who has not worked in the consular department for some time, should not have access to NVIS. As for the role [CONFIDENTIAL], the AP follows the BZ's opinion that the finding in this regard had an incorrect reference to the source. The concerned finding related to employees of CSO and has corrected the AP above with appropriate source corrected.

136. Finally, the AP established during the investigation that a statement of reasons for granted incompatible roles within NVIS is missing. In its view, BZ states that in certain cases, there is no may be that conflicting roles are assigned to a person. This could be, for example, smaller posts where an employee suddenly drops out. According to BZ, the motivation of conflicting roles are documented. As a result, the AP has requested documentation about the responsibility and motivation for assigning incompatible roles. Based upon this the AP notes that BZ has shown several examples showing that BZ plays incompatible roles in the past.124 With regard to this point, the AP follows the view of the Ministry of Foreign Affairs. The AP has cannot, however, see a policy showing how BZ deals with incompatible roles and how BZ incompatible roles. The NVIS Data Management Manual only states that the incompatible roles in NVIS are currently not established.125 Policy regarding segregation of duties is ideally suited to

to be included in the security policy as referred to in paragraph 2.3.

137. In view of the above, the AP is of the opinion that BZ, with regard to procedures regarding access rights to the NVIS environment and its control, violates Article 32(1) of the GDPR and further elaborated in 32, paragraph 2, under f and k, VIS Regulation and BIO standards 9.2.1, 9.2.2, 9.2.5 and 9.2.6. (and relevant standards from the BIO about the Plan-Do-Check-Act cycle).126

123 E-mail BZ to the AP of 9 January 2022, BZ process NVIS authorization.

124 E-mail BZ of 10 December 2021, appendix 20 and 20.1 and the written Opinion BZ of 15 October 2021, appendix 22.

125 File 3, appendix 1: NVIS Data Management Manual February 2018, p. 16.

126 This means that it must be regularly checked whether the security policy is still being observed in practice and whether the measures are still being taken to fulfil. Should imperfections come to light, the Plan-Do –Check-Act principle from the BIO – in short – requires that errors

2.6 NVIS Usage Monitoring: Log Files

2.6.1 Legal framework

138. The obligation to maintain and regularly check logs is an essential part of the information security regulations. In this way an organization can see keep track of which employee consults or changes certain information when and for what purpose. It is

139. In addition, it is necessary that periodic monitoring of the recorded log files takes place in order to detect unusual patterns and, for example, check whether unauthorized access to the data takes place.

Article 32(2)(i) and (k) of the VIS Regulation provides that BZ must be able to verify and determine

which personal data are processed in NVIS when, by whom and for what purpose. BZ must also de

verify the effectiveness of these security measures and, with regard to internal control, the

take necessary organizational measures. Article 32(2)(f) of the VIS Regulation requires that

those authorized to consult the VIS have access only to the data on which

their access authority, and solely with personal and unique

user identities and secret access procedures (data access control).

140. The BIO standards prescribe that BZ log files with the registration of activities of NVIS

users and review these logs regularly. The BIO standards

specify the minimum information about NVIS usage that should be kept in a log file

registered. BZ must also have an overview of all log files that are used in the context of NVIS

generated. In the BIO, the following regulations are particularly relevant:

Log events

Event logs that record user activity, exceptions

and record information security events should be

be created, stored and regularly reviewed.

A log line contains at least:

a. the event;

b. the necessary information needed to determine the incident with a high degree of certainty

trace back to a natural person;

c. the device used;

d. the result of the action;

e. a date and time of the event.

There is an overview of log files that are generated.

12.4.1

12.4.1.1

12.4.2.1

be rectified and that the policy is adjusted in such a way that the problems in question will not recur next time. The

The results of the on-the-spot check by AP inspectors described above show that this has not happened with regard to authorizations and role management. As a result, there is no appropriate internal control in the field of access security. This may result in

the risk of access to NVIS for unauthorized persons, as referred to in Article 32 paragraph 2 under b VIS Regulation.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

2.6.2 Factual Findings

141. In order to verify compliance with legal requirements regarding log files, the

AP requested a sample of the log files from BZ. These log files contain logs from the

consular posts, from CSO and from Processor 2. During the on-site investigations, the AP also 127

questions about the organization of the logging and the internal control of this by BZ. Furthermore, the AP

checked the requested log files and compared them with the corresponding

authorization lists relating to the same period.

Logging of NVIS usage at consular posts London and Dublin

[CONFIDENTIAL]

[CONFIDENTIAL]128

Log file analytics

142.

143.

144. The AP has requested two log files regarding the NVIS use by the employees

from the Consular Post in London. The first file (hereinafter referred to as: Log 1) concerns the log file of 4

July 2019, between 9.00 and 12.00. This period coincides with the investigation by the AP on the spot. It

The second file (hereinafter: Log 2) covers the period from April 1 to July 4, 2019.

[CONFIDENTIAL]129

[CONFIDENTIAL] 130

145.

146.

127 On-site investigations at the consular post London (2 and 4 July 2019), the CSO The Hague (18 July and 12 September 2019), Processor 2 (1 November 2019) and the Dublin consular post (22 and 23 January 2020).

128 Written Opinion BZ dated 15 October 2021, appendix 2 under number 6.3.

129 File 12, appendices 40a and 40b: Logging use of NVIS, version 25 July 2019 and Explanatory notes.

130 File 16, appendix 8.1: LON_01April2019_04July2019_Overzicht.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

Logging of NVIS usage at CSO The Hague

During the on-site investigation at the CSO131, the AP conducted interviews with the employees of BZ about the various aspects of security with regard to NVIS, whereby the subject 'logging of NVIS' has been investigated. The AP also has additional documentation on this subject at BZ retrieved132 and analysed. In addition, the AP performed analyzes of log files.

Process of logging and checking log files

[CONFIDENTIAL]133

[CONFIDENTIAL] 134 135

147.

148.

149.

131 File 11: Report of Official Acts OTP CSO 18 July 2019 and 12 September 2019.

132 File 13: AP information request of 25 July 2019; and File 17: AP information request of 1 October 2019.

133 File 11: Report of Official Acts OTP CSO 18 July 2019 and 12 September 2019.

134 File 13: AP information request of 25 July 2019.

135 File 14, appendix 18.1: Responsibility for checking NVIS use.

150. The AP has requested (extensive) documentation in the field of security from BZ and analyzed for relevant information about logging. The AP has focused on information about logging the actions within the NVIS platform, in particular how the logging process and control thereof are set up, which log files are generated, and how log files are checked. It concerns the following documents: [CONFIDENTIAL];136 [CONFIDENTIAL];137 [CONFIDENTIAL]; 138 [CONFIDENTIAL];139 [CONFIDENTIAL];140 [CONFIDENTIAL].141

[CONFIDENTIAL]

Log file analytics

151.

152. The AP has also requested log files from NVIS from BZ in which the NVIS actions of the

153.

154.

employees of the CSO are recorded. BZ has submitted the following log files to the AP that relate to the following periods:

(1) September 1, 2018 through November 30, 2018; (hereinafter: Log 3);142

(2) April 1 to July 18, 2019, (hereinafter: Log 4);143

(3) on September 12, 2019 (hereinafter: Log 5).144

[CONFIDENTIAL]

[CONFIDENTIAL]145

136 File 14, appendix 14.1: [CONFIDENTIAL]

137 File 12, appendix 44b: [CONFIDENTIAL]

138 File 14, appendix 16.1: [CONFIDENTIAL]

139 File 14, appendix 16.2: [CONFIDENTIAL]

140 File 14, appendix 19.1: [CONFIDENTIAL]

141 File 14, appendix 19.2: [CONFIDENTIAL]

142 File 16, appendix 9.1: CSO_01Sept2018_30Nov2018_Overzicht.

143 File 16, appendix 9.2: CSO_01April2019_18Juli2019_Overzicht.

144 File 16, appendix 9.3: CSO_12Sept2019_Overzicht.

145 Written Opinion BZ of 15 October 2021, p. 10 and 11.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

Processor 2

[CONFIDENTIAL]

[CONFIDENTIAL]146

[CONFIDENTIAL]147

155.

156.

157.

158. Finally, the AP analyzed some log files from Processor 2. The AP establishes that, because of the lack of sufficient evidence about the factual situation in combination with the explanation from BZ, for what regarding the content of these log files cannot determine a violation and will therefore not continue in the legal assessment below.148

2.6.3 Legal Assessment

159. The AP has assessed to what extent BZ has taken appropriate measures in the field of logging of the NVIS environment.

160. The AP notes that log files are kept with regard to NVIS. In the log files the names of employees are registered and only a very limited amount of other data with related to actions in NVIS, such as an indication of some steps under the visa process (eg [CONFIDENTIAL]).

146 File 13: AP information request of 25 July 2019; and File 15: AP information request of 1 October 2019 and announcement OTP Processor 2 on November 1, 2019.

147 File 17: Report of Official Acts OTP Processor 2 1 November 2019, p. 7 and 8.

148 Written Opinion BZ of 15 October 2021, p. 11.

161. Log 1 does not show which actions are performed in NVIS by the employees of the consular post in London performed and at what time. With regard to Log 2, AP determines that it cannot be verified which data of visa applicants have been processed by the consular post staff, with which purpose, when this took place and which device was used. The AP states

In addition, note that there are discrepancies between the two log files. Since Log 1 is about July 4, 2019 and

Log 2 over the period July 1, 2019 to July 3, 2019, Log 2 and Log 1 are chronologically related.

However, both files differ in their structure.149

In Log 3, Log 4 and Log 5, in addition to the name of the employee, you will also find the visa application number and a global indication of the part of the visa process that has been carried out and the time when part has been completed. However, these log files do not show which personal data of visa applicants have processed the employees of the CSO, for what purpose and at what time this occurred.

162.

163. In view of the findings above, the AP concludes that BZ does not have an adequate overview of the log files generated in the NVIS environment. Although NVIS usage is logged, but the submitted log files show in terms of structure and type of data contained therein inconsistencies.150 The log files received and reviewed by the AP also show that not all mandatory actions are logged. [CONFIDENTIAL]151

In its opinion (in so far as it is still relevant to the violation) BZ states the next one. With regard to log file 1, according to BZ, it would have been on the way of the AP to put BZ on it point out that not only the access log data was requested, but also what actions in NVIS were performed and at what time. This argument fails. In its request for information, the AP has included a log file asked about the use of NVIS at the embassy in London.152 In the opinion of the AP little argument that when using NVIS, in which - undisputed - personal data are processed, the AP is not only interested in information about logging into this system.

164.

165. With regard to log file 2, BZ states that Article 32 paragraph 2 under i of the VIS Regulation, to which AP logging requires that it be recorded what data is being processed. But this article does not require that every data that is processed is logged. An indication of what data is being processed can therefore suffice, according to BZ, without an exact representation of those data. Meaning is added to Article 32 GDPR. The purpose of the logging is to check for legitimate use of access rights. Because

BZ records which application data is processed, it is therefore sufficiently precise which

data has been processed. According to the Ministry of Foreign Affairs, the visa application number also makes it possible to

identify the person concerned

personal data has been processed. It would be going too far to have it recorded per visa applicant whether the

For example, NVIS employee has processed only the name or only the date of birth or both.

149 The differences concern the number of logged variables and their names in the log files.

150 For example, compare the type of actions recorded in Log 1 with the type of actions recorded in Log 2.

151 Information provided by BZ during OTP's CSO on 16 July 2019 and 12 September 2019 (see file document 11: Report of

OTP Official Acts

CSO July 16, 2019 and September 12, 2019).

152 File 10, appendix 1 under item 40.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

166. The AP does not follow BZ's view. Article 32 paragraph 2 under i of the VIS Regulation requires that the

it must be possible to verify and establish which data is collected when, by whom and for what purpose

processed in the VIS. Logging a visa application number does not provide sufficient information about which

data is processed. This means that afterwards it is not possible to see which data has been processed and when.

The more sensitive the personal data that is processed is, the higher the requirements for logging in this regard

to be. In this context, where a great deal of – including – special personal data is processed, it is of

It is very important that changes in data can be traced back. BZ must be able to check which data

by whom changed, not just after an incident. This information may also be from a combination of

(log) files are derived. The purpose of logging is thus not limited, as BZ states, only to the

checking the lawful use of access rights.

In its written opinion, BZ further states that the conclusion of the AP that checks on the NVIS use that BZ carries out are aimed at the granted authorizations and not at log files and actions performed in NVIS by employees is incorrect and premature. BZ is of the opinion that it request for information about this was formulated too generally by the AP. According to BZ, there are many possibilities to make reports on the actual use of NVIS. Finally, BZ states that the question from the AP was unclear about logging and how the control of this was in the security policy tuned.

167.

168. Although the AP is of the opinion that it is up to the Ministry of Foreign Affairs to timely - and not only in an opinion - to indicate that a request for information raises questions, the AP BZ once again has the opportunity to submit procedures that describe how BZ logs with regard to NVIS and performs checks on this.153 In response to this, BZ has an undated document with a few paragraphs provided with a factual description of what is logged when using NVIS.154

[CONFIDENTIAL]155

169. Given the deficiencies in log files in combination with the fact that BZ does not regularly assesses and there is no procedure in this regard, the DPA concludes that BZ in contravenes Article 32(1) of the GDPR and further detailed in Article 32(2)(f), i and k of the VIS Regulation and the BIO standards concerning log files (in particular standard 12.4.1).

2.7 NVIS Usage Control: Security Incidents

2.7.1 Legal framework

Article 32(2)(c) and d of the VIS Regulation respectively provide that BZ must takes measures to prevent data carriers from being illegally read, copied,

170.

153 Letter from AP to BZ dated 19 November 2021, p. 3.

154 E-mail BZ to AP of 10 December 2021, annex 16.

155 See paragraph 2.6.2 and letter from the Ministry of Foreign Affairs to AP dated 19 November 2021, appendix 1 Interview

changed or deleted, and that data is illegally viewed, changed or deleted. In the event that there is unauthorized (external or internal) access to data carriers and/or personal data stored in the NVIS environment, then there is a security incident. Under the requirements of Article 32(2)(k) VIS Regulation applies that the necessary organizational measures have been taken should be used for the follow-up of such security incidents. These provisions therefore write before internal checks on the NVIS data carriers and the storage of NVIS data must take place and that the effectiveness of the security measures should be checked.

Chapter 16.1 of the BIO describes the mandatory standards for the management of the security incidents and improvements. This includes the following BIO standards from application:

16.1.1 1

16.1.2

16.1.2.1

16.1.2.2

16.1.2.3

16.1.2.5

16.1.2.6

16.1.3

16.1.6

16.1.6.1

Responsibilities and Procedures:

Management responsibilities and procedures should be established to

rapid, effective and orderly response to information security incidents

accomplish.

Information security event reporting:

Information security events should be handled as quickly as possible through the appropriate

management levels to be reported.

There is a reporting desk where security incidents can be reported.

There is a reporting procedure that sets out the tasks and responsibilities of the reporting desk

described.

All employees and contractors have verifiably taken note

of the incident reporting procedure.

The process owner is responsible for resolving security incidents.

Follow-up of incidents is reported monthly to the responsible person.

Reporting information security vulnerabilities:

From employees and contractors who use the information systems and

the organization's services should be required to provide the information contained in systems or services

register perceived or suspected vulnerabilities in information security and

report.

Lessons learned from information security incidents:

Knowledge gained by analyzing information security incidents

and to solve should be used to determine the probability whether

reduce the impact of future incidents.

Security incidents are analyzed for the purpose of learning and

prevent future security incidents.

171.

The above BIO standards indicate that a consistent and effective approach should be

be accomplished in the management of information security incidents, including

communication about security events and security vulnerabilities. serve this purpose

responsibilities and procedures to be established, a reporting point to be set up, in which

security incidents are reported, including the reporting procedure. Information security incidents and

the follow-up of this is reported to the responsible person on a monthly basis. For this,

172.

security incidents, among other things, with the aim of learning and future

prevent security incidents.

2.7.2 Factual Findings

In the context of its investigation, the AP has checked whether BZ has a procedure for

reporting and following up on security incidents/data breaches in relation to NVIS and the visa process. In that

In connection with this, the AP BZ has asked for an extract from the notification register for 2018 and 2019 in which all

NVIS-related security incidents are registered. During the investigation, the AP

inspectors about this and the relevant documentation about security incidents

requested.

Consular posts: London and Dublin and CSO The Hague

Procedure for security incidents

173. The consular posts in London and Dublin and the CSO follow the same BZ-wide approach with regard to

174.

to report security incidents/data breaches: a security incident is reported immediately

[CONFIDENTIAL] reported, and if there is a data breach, a [CONFIDENTIAL]

created and sent digitally to [CONFIDENTIAL]. This procedure is set to [CONFIDENTIAL],

to be consulted by BZ staff [CONFIDENTIAL].

On site at the consular posts, employees also make use of 'Data breach factsheets' that are available in the

Dutch and English have been drawn up. These fact sheets are a schematic representation of the procedure

with a summary of all steps that employees must follow in the event of a data breach.

During the investigations, the aforementioned fact sheets data leaks were shown to the AP inspectors

[CONFIDENTIAL].

175. Following the investigation in London, the AP asked BZ156 to report the procedure

provide data breaches. BZ has submitted the following documents:

-

-

Factsheets data breach August 2018157, both in Dutch and English. See these fact sheets

on the schematic representation of the working method in the event of data breaches, as described above and

displayed at the consular posts.

Instructional videos about data breaches158: these short films provide information about

data leaks.

- Printout of the information material about data breaches on [CONFIDENTIAL], with examples

of data breaches159 and the description of the working method for BZ employees in the event of

data leaks160. This last document contains a description of the steps that employees of

156 File 10: AP information request of 12 July 2019.

157 File 12, appendix 11a: Factsheet data breach NL Aug 2018; File 12, appendix 11b: Factsheet data breach EN Aug 2018;

and

File 12, appendix 11d: Sharepoint data leaks.

158 File 12, appendix 11c: Instruction video - Help, a data breach; and File 12, appendix 11f: Data breach movie. These file

documents are

video files.

159 File 12, appendix 11e: Data leaks examples sharepoint.

160 File 12, appendix 12c: Data leaks information for BZ employees.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

BZ must take in the event of data leaks, in accordance with the procedure that was followed during the studies in London and Dublin has been explained.

176. The AP notes that the employees of the consular posts in London and Dublin and the CSO, including regarding reporting security incidents/data breaches, follow the procedure for all BZ employees. This procedure is a practical guide to the steps that employees must take action in the event of security incidents: these must be addressed as soon as possible [CONFIDENTIAL] are reported and in the event of data breaches, a report will be made to [CONFIDENTIAL]. The said procedure has not been established at a management level, and gives further no insight into the steps that are followed after a report about a security incident/ data breach has occurred. The procedure also does not describe the duties and responsibilities of the reporting desk and who, as process owner, is responsible for resolving security incidents and the report on this.

Security Incidents

[CONFIDENTIAL]

177.

179.

178. The AP has requested a security incident register from BZ161 in which all security incidents in relationship to NVIS and the visa process are listed, with respect to the following periods: (1) October 1

2018 through December 31, 2018, and (2) April 1, 2019 through July 1, 2019. The AP has nine notifications of incidents162 at the London consular post. [CONFIDENTIAL]. By the lack of during the investigation, the AP was under the assumption that BZ has not provided a copy of the security incident register.

[CONFIDENTIAL]163

[CONFIDENTIAL] 164

180.

161 File 10: AP information request of 12 July 2019.

162 [CONFIDENTIAL]

163 [CONFIDENTIAL]

164 File 11: Report of Official Acts OTP CSO 18 July 2019 and 12 September.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

181.

182.

An employee of [CONFIDENTIAL] stated during the investigation that BZ had incident register in which security incidents are registered. The AP has asked to provide a security incident register related to NVIS and concerning the year 2018 and the first half of 2019. [CONFIDENTIAL]165. BZ has not supplied a (blank) incident register. In addition, the AP has also asked for a six-monthly report on security incidents. This document has been provided.166 It describes data leaks related to travel documents.

During the opinion phase, BZ provided, among other things, the following explanation about the process of: security incidents. Reports are handled by [CONFIDENTIAL] in [CONFIDENTIAL].

All actions required to handle a report are recorded herein and

stored. These reported incidents/violations, regardless of whether they had been reported to the AP

must be completed, closed, logged and stored in a

protected area accessible only to [CONFIDENTIAL] behind the [CONFIDENTIAL]

(the data leak register). All performed (follow-up) steps are recorded in the individual

reporting files in the central register of incident reports that is filled by

[CONFIDENTIAL]. Finally, BZ has stated that all incidents are now in one central place

are tracked and stored.

183. As a result of the foregoing, BZ has answered further questions from the AP about the design

of the central register of security incidents. Based on this and on the basis of the above

explanation, the AP considers it sufficiently plausible that BZ does have a

security incident register in which security incidents in relation to NVIS are registered.

Processor 2

184. On November 1, 2019, the AP conducted an investigation at Processor 2. The AP hereby has the

received the procedure that Processor 2 uses in the event of security incidents.167 In this

escalation procedure describes which steps must be taken within the organization

when a security incident occurs, which roles/functions should be assigned to Processor 2

informed and to which roles/functions should be escalated. Processor 2 also has a policy

submitted that pertains to security incidents168 and data leaks169.

185. With regard to security incidents, Processor 2 stated during the investigation that in 2018

and 2019 there have been no incidents in relation to the NVIS environment. This looked specifically at incidents

[CONFIDENTIAL]

165 File 14, appendix 20.1: Explanation.

166 File 14, appendix 21.1: [CONFIDENTIAL].

167 File 17, Appendix 3: Incident Escalation Procedure.

168 File 17, Appendix 4: [CONFIDENTIAL].

169 File 17, appendix 5: Data Breach Controller procedure.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

186. When asked whether Processor 2 maintains a log or registry of security incidents, Processor 2 stated to use different registers depending on the incident. Processor 2 has explained that two incident registers are used.

[CONFIDENTIAL]170 171

[CONFIDENTIAL]. Processor 2 has indicated that there are no security incidents at Processor 2 related to NVIS during the study period. As a result, there were no internal reports which Processor 2 could provide to AP.172

187.

188. On the basis of the above and the explanation provided by BZ during the opinion phase, the AP deems the division of tasks between BZ and Processor 2 with regard to security incidents is sufficiently clear.

2.7.3 Legal Assessment

189. The AP concludes that the general procedure provided by BZ at the time of the investigation for reporting security incidents by BZ employees is not sufficient. This procedure is a no more than a manual on the steps employees should take when security incidents: these must be reported to [CONFIDENTIAL] as soon as possible and in case data leaks will be reported to [CONFIDENTIAL]. The mentioned procedure is not on management level and provides no further insight into the specific steps that are followed after a report about a security incident/data breach has taken place. The procedure describes also not the tasks and responsibilities of the reporting desk and who is responsible as process owner is for resolving security incidents and reporting them.

During the opinion phase, BZ issued a GDPR manual in response to this (approved on 13 October 2021) and a Process Description Incident Management Security Incidents and Data Breach (July 2020) provided to the AP. The AP has reviewed this documentation and has come to the conclusion that BZ from 13 October 2021 provides full insight into the steps that are followed after a report about a security incident/data breach has occurred. Also, the duties and responsibilities of the reporting desk and the Ministry of Foreign Affairs has established who, as process owner, is responsible for the resolving security incidents and reporting on them.

190.

170 File 23, appendix 06.2: Notes to the Incident Register October 2018 up to and including 1 November 2019.

171 File 23, appendix 06.1: -AP-z2019-12207-06-Incident Register extract.

172 Written Opinion BZ of 15 October 2021, p. 13.

191. On the basis of the above, the AP concludes that BZ, with regard to the defects in the procedure for reporting security incidents, until 13 October 2021 insufficiently appropriate has taken organizational measures to prevent unlawful data processing in NVIS. As a result, BZ has infringed the requirements laid down in Article 32(1) of the GDPR and further elaborated in Article 32, paragraph 2, under c and d, of the VIS Regulation and the BIO standards 16.1.1 and 16.1.2.2. As of October 13, 2021, the aforementioned defects have been repaired by BZ and the infringement of this point ended.

2.8 Training personnel on the protection of personal data

192. Article 28(5) VIS Regulation requires that the staff of the authorities with right of access to the VIS should receive proper training on data security and protection rules.

Staff are also informed of relevant criminal offenses and sanctions. the AP
however, has not tested the content of these courses nor the way in which they are offered
during the investigation. Article 38(3) of the Visa Code further stipulates that the 'central authorities of
Member States [should] provide appropriate training for both posted and local staff and
provide them with complete, accurate and up-to-date information on the relevant legislation."

193. The AP establishes on the basis of the statements of employees and the documents provided by BZ
with regard to training employees who have access to data in the NVIS that there is
of training in data protection and security. In addition, the courses
offered to employees who have only been employed for a short time and employees who have been with BZ for a longer
period of time
to work. The courses include, among other things, the systems to be used (including NVIS), relevant laws and
regulations and security. The AP also notes that there are training courses from both posted and
local employees.

194. With regard to the question of whether attention is paid to
information security and regulations regarding the processing of personal data, compliance with requirements
that are laid down in BIO objective 7.2.2 and Article 38, paragraph 3, Visa Code.

2.9 Information provision to visa applicants

2.9.1 Legal framework

Being transparent about data processing is one of the general principles for a proper
data processing. Informing the data subject about data processing contributes to
transparency. Article 37 VIS Regulation requires visa applicants to be informed about the
controller, the purposes of the processing of the personal data of the visa applications, the
categories of recipients of processed personal data, the retention period, the obligation of the
collecting this data and the rights of the data subject. This means that BZ will grant visa applicants

195.

in writing when collecting the data for the application form, the photo

and fingerprints.173 This obligation also derives from Article 13 of the GDPR.

2.9.2 Factual Findings

196. The AP conducted an investigation at the consular post in London and Dublin. From these studies

and the information obtained follows, that data subjects can be informed in three ways about

processing their photos, fingerprints and personal data for the purpose of a visa application.

Information is provided through (1) a “Privacy statement regarding Short-Stay Visa”

Applications” (hereinafter: Privacy Statement)174, (2) an appendix to the application form for the

visa application (hereinafter: Annex)175, and (3) a folder176 at the location of the consular post.

197. The first option for providing information is the Privacy Statement. On the (in English

198.

written) websites of the embassies in Ireland and the United Kingdom contain information about the

ask how a (Schengen) visa application works. 177 The websites refer to this Privacy

Statement, which can be found on the website of BZ.178

Various privacy components are discussed in the Privacy Statement, such as the goals for the

processing of the personal data of the visa applications, the controller, the

retention period of 5 years, the obligation to collect the data and the rights of

involved. A separate document lists the risk countries that could have an impact on the

visa process regarding risk analyses.179 The Privacy Statement further states that there may be

sharing personal data with third parties such as other European authorities within the Schengen area

area and bodies such as Europol. The Privacy Statement does not mention the possible

processors of personal data such as, for example, private parties that may be involved in the

process of visa applications. The AP further notes that the national “Data Protection Authority”,

including the address details, is mentioned in the privacy statement as the designated body in the

case the data subject would like to exercise her/his rights.180

199. The second possibility of providing information takes place via the Annex.181 The Annex is

provided in writing to the data subject at the time the details of the application form are

collected. In the Appendix BZ is mentioned as the controller for the

data processing, the purposes of the processing of personal data are stated, the

retention periods and the obligation to collect the personal data

173 Article 37(2) Regulation “The information referred to in paragraph 1 shall be communicated in writing to the applicant when the

details of the application form, the photograph and the fingerprint data as referred to in Article 9(4), (5) and (6).”

174 File 7, Appendix 2: Privacy Statement re. Short stay visa applications.

175 File 7, Annex 6: Schengen Visa Application (sample form), provided for the attention of the OTP consular post in London.

176 File 7, Annex 4: Information sheet on SIS II; and Dossierstuk 27, appendix 10: Public information folder about SIS II.

177 For Ireland, see:

https://www.netherlandsandyou.nl/your-country-and-the-netherlands/ireland/travel-and-residence/applying-for-a-short-

stay-schengen visas (last accessed 14 August 2020) and for the United Kingdom:

https://www.netherlandsandyou.nl/your-country-and-the-netherlands/united-kingdom/travel-and-residence/applying-for-a-short-stay-

schengen visas (last accessed August 14, 2020).

178

https://www.netherlandsandyou.nl/documents/publications/2017/12/06/privacystatement-regarding-short-stay-visa-applications-en (for

last accessed on February 23, 2022).

179 In accordance with Article 22 Visa Code.

180 Article 37(1)(f) VIS Regulation.

181 File 7, Annex 6: Schengen Visa Application (sample form), provided for the attention of the OTP consular post in London.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

explained. Reference is also made to the Dutch Data Protection Authority for complaints handling.

The AP further notes that permission is requested from the data subject. In the list of categories

of recipients of personal data are not referred to as third private parties.

200. The third possibility of providing information emerged from the Dublin investigation,182 when the

employees of the consular post have been shown a folder SIS II183 that is made available to the

visa applicants in the waiting area. This leaflet relates to SIS II and does not contain information about

rights of data subjects with regard to a visa application and the exercise of rights of data subjects

during the visa application process. While the leaflet itself is informative on SIS II against the

background of the visa application, the folder is not applicable with regard to exercising

rights of data subjects in the visa process.

2.9.3 Legal Assessment

201. The AP has established that BZ sets out the purposes of the data processing in the Privacy Statement and in the Annex

(1)

mentions, (2) makes it clear that the collection of the data is mandatory, (3) includes retention periods,

and (4) names the competent (privacy) supervisor.184 However, with regard to both documents,

not all (categories of) recipients of personal data are listed by BZ. The AP determines

that only a few categories of recipients have been mentioned, such as other European authorities and Europol.

The Privacy Statement and the Appendix make no mention of sharing personal data with third parties

private parties, such as processors Processor 2 and Processor 3 that are involved in the process of the

visa application. This does not meet the requirement of Article 37(1)(c) of the VIS Regulation and Article

13(1)(e) GDPR.

202. In its view, BZ states that it is not a foregone conclusion that data subjects must be informed about the provision of data to a processor. BZ is of the opinion that Processor 2 only as processor qualifies and not as a recipient of personal data. Without the obligation to do so acknowledge that BZ will include in the Privacy statement and/or the Appendix that BZ leaves personal data processing by processors.

203. The AP does not follow BZ's argument. It follows from Article 13(1)(e) of the GDPR that the controller informs the data subject about the recipients or categories of recipients of the personal data. Article 4(9) GDPR defines a recipient as a natural or legal person, public authority, agency or other body, whether or not a third party to whom/to whom the personal data is provided. Processors as Processor 2 and Processor 3 are legal entities that receive the personal data about the data subjects. The Guidelines on transparency also state that a recipient can be a processor.185

182 File 27: Report of Official Acts OTP consular post Dublin.

183 File 7, Annex 4: Information sheet on SIS II; and Dossierstuk 27, appendix 10: Public information folder about SIS II..

184 However, the Appendix still refers to the Dutch Data Protection Authority.

185 Article 29 Data Protection Working Party Guidelines on transparency pursuant to Regulation (EU) 2016/679, p. 18.

2.10 Conclusions

204. The AP comes to the following conclusions with regard to the established violations.

Security plan

205. The AP comes to the conclusion that BZ does not have a security plan with regard to NVIS (and therefore this too

has not evaluated). BZ has acted in violation of this at least from 1 September 2018 to the present

Articles 24 and 32(1) of the GDPR, which is further elaborated in Article 32(2), preamble, VIS Regulation and BIO-standards 5.1.1, 5.1.1.1 and 5.1.2.1.

Physical Security

206. By not explicitly determining which parts of the IT infrastructure should be designated, BZ has become the critical infrastructure of the visa process, from at least September 1, 2018, until at least case in the spring of 2020 acted contrary to Article 32(1) of the GDPR, which is further elaborated in Article 32(2)(a) VIS Regulation.

207. The AP also comes to the conclusion that BZ, when it comes to drawing up emergency plans and the protection of equipment against disruptions in utilities, from at least September 1, 2018 to date does not comply with the provisions of Article 32(1) of the GDPR, which has been further elaborated in Article 32(2) thereof sub a, VIS Regulation and organic standards 11.1.4 and 11.2.2.

208. Furthermore, the AP is of the opinion that due to the lack of security guarantees when entering the zone that must be extra secured, the physical security of the areas in which work is carried out on the visa process in London was not satisfactory. As a result, BZ has from at least September 1, 2018 to April 2020, acted contrary to Article 32(1) of the GDPR, which is further elaborated in Article 32(2)(a) VIS Regulation and BIO standards 11.1.1 to 11.1.5 and 11.2.2.

209. Finally, since the Ministry of Foreign Affairs has not demonstrated that there are sufficient guarantees for the physical security at working in NVIS in public spaces and BZ also does not have the effectiveness of the policy in this regard checked, the AP comes to the conclusion that BZ is in conflict from at least September 1, 2018 to the present acts in accordance with Article 32(1) of the GDPR, which is further elaborated in Article 32(2)(a) and (k) of the VIS Regulation.

Access rights to NVIS

210. The AP comes to the conclusion that from at least September 1, 2018 to January 1, 2022, BZ does not have formal registration and opt-out procedures with regard to the allocation of access rights to

NVIS. In doing so, BZ has acted in violation of Article 32(1) of the GDPR, which has been further elaborated in BIO-standards 9.2.1 and 9.2.2.

211. The AP is also of the opinion that BZ, with regard to the procedure regarding the control of access rights to the NVIS environment and its control in practice, from at least September 1, 2018 to the present in contravenes Article 32(1) of the GDPR which is further elaborated in 32(2)(f) and (k) of the VIS Regulation and BIO standards 9.2.1, 9.2.2, 9.2.5 and 9.2.6.

Control NVIS usage: logging

212. In view of the deficiencies in log files in combination with the fact that BZ does not regularly assesses and there is no procedure in this regard, the DPA concludes that BZ van at least September 1, 2018 to date does not comply with Article 32(1) of the GDPR that is further elaborated in Article 32, paragraph 2, under f, i and k of the VIS Regulation and the BIO standards concerning log files (in particular standard 12.4.1).

NVIS Usage Control: Security Incidents

213. With regard to the deficiencies in the procedure for reporting security incidents, the AP comes to the conclusion that BZ from at least September 1, 2018 to October 13, 2021 is insufficiently appropriate has taken organizational measures to prevent unlawful data processing in NVIS. As a result, BZ has infringed Article 32(1) of the GDPR, which has been further elaborated in Article 32, paragraph 2, under c and d, VIS Regulation and the organic standards 16.1.1 and 16.1.2.2.

Information provision to visa applicants

214. Finally, the AP concludes that BZ, in the context of the provision of information, visa applicants do not disclose the sharing of personal data with third private parties,

such as Processor 2 and Processor 3. With this BZ violates from at least September 1, 2018 to the present

Article 13(1)(e) of the GDPR which is further elaborated in Article 37(1)(c) of the VIS Regulation.

3 Fine

215.

216.

217.

3.1 Introduction

BZ has acted in violation of Article 32(1) of the GDPR and Article 13(1)(e) of the GDPR. As a result, BZ . has

not acted in accordance with the basic principles of the processing of personal data

as referred to in Article 5 of the GDPR. The AP uses its for the detected violations

authority to impose a fine on BZ. In its opinion, BZ has stated that various

transition processes and improvement measures the imposition of a fine and/or order subject to periodic penalty payments not

is reasonable. Due to the seriousness of the violations, the extent to which they can be blamed on BZ and

the fact that the violations are still continuing, the AP, unlike BZ, considers the imposition of a fine and a

charge under duress is appropriate. The AP justifies this in the following.

3.2. Fine policy rules of the Dutch Data Protection Authority 2019

Pursuant to Article 58, second paragraph, preamble and under i and Article 83, fourth paragraph, of the GDPR, read in

in conjunction with article 14, paragraph 3, of the UAVG, the DPA is authorized to give BZ the authority in the event of a

violation

of Article 32 of the GDPR to impose an administrative fine of up to € 10,000,000.

Pursuant to Article 58, second paragraph, preamble and under i and Article 83, fifth paragraph, of the GDPR, read in

in conjunction with article 14, paragraph 3, of the UAVG, the DPA is authorized to give BZ the authority in the event of a violation

of Article 13 of the GDPR to impose an administrative fine of up to € 20,000,000.

218. The AP has established fine policy rules regarding the interpretation of the aforementioned power to

imposing an administrative fine, including determining the amount thereof.186 In the

Fines policy rules have been chosen for a category classification and bandwidth system. Violation of

Article 32 of the GDPR is classified in category II. Category II has a penalty bandwidth between €

120,000 and €500,000 and a basic fine of €310,000. Violation of Article 13 of the GDPR is classified

in category III. Category III has a fine range between €300,000 and €750,000 and a basic fine

from € 525,000

219. The AP adjusts the amount of the fine to the factors referred to in Article 7 of the

Penalty policies, by decreasing or increasing the base amount. It is an assessment of the

seriousness of the violation in the specific case, the extent to which the violation can be attributed to the offender

be blamed and, if there is reason to do so, other circumstances.

3.3 Fine for breach of the security of the processing

220. Any processing of personal data must be done properly and lawfully. To prevent

organizations with the processing of personal data infringe the privacy of citizens it is of

186 Stct. 2019, 14586, March 14, 2019.

It is very important that they apply a risk-adjusted level of security. When determining the risk

for the data subject include the nature of the personal data and the scope of the processing

important: these factors determine the potential harm for the individual involved in, for example,

loss, alteration or unlawful processing of the data. As the data becomes more sensitive
character, or the context in which they are used, pose a greater threat to personal
privacy, stricter requirements are imposed on the security of personal data. The
AP has concluded that BZ does not have a sufficiently risk-adjusted security level
guaranteed and guaranteed in the context of processing Schengen visa applications.

3.3.1 Nature, seriousness and duration of the infringement

221. The AP has established that BZ processes a great deal of (sensitive) personal data of those involved.
Examples of this are the combination of name and address details, country of birth, purpose of the trip,
nationality and photo. Data subjects are obliged to provide all these personal data to BZ in order to
to obtain a Schengen visa. In such a dependent and unequal position it is of
It is very important that BZ sufficiently guarantees and guarantees a level of security that is appropriate to risk. The
consequences and the resulting damage for those involved are large in the event of loss,
modification or unlawful processing of the data. For example, unauthorized persons can
view and change personal data, but authorized employees can also
make input errors of the request. As a result, applications can be wrongly refused, which again
constitutes an infringement of the freedom of movement of the data subjects. The AP therefore concludes that as a result
of the circumstance that BZ has failed to take appropriate technical and organizational measures
the confidentiality and integrity of the personal data are insufficiently guaranteed.

222. In addition, the AP takes into account that BZ processes personal data of a large number of data subjects.
It is established that BZ processes hundreds of thousands of applications per year (682,484 in 2018, 739,248 in 2019 and
169,926 in 2020).187 The personal data of all these applications are therefore insufficiently secured. Finally
the AP notes that the violation has been going on for 3.5 years and is still ongoing. The AP considers this
extremely serious.

223. In view of the above, the AP sees, on the basis of Article 7, opening words and under a, of the Fine Policy Rules
reason to impose a fine on BZ and to increase the basic amount of the fine from €310,000 to €
390,000.

3.3.2 Negligent nature of the infringement

224. BZ is obliged to maintain a security level that is appropriate for the nature and scope of the processing carried out by BZ. Now that BZ has not guaranteed an appropriate level of security for years, the AP of believes that BZ has been and continues to be seriously negligent in taking appropriate security measures and checking and adjusting these measures. Citizens who are obliged to hand over personal data, must be able to assume that BZ, as a government agency, will has taken and takes the necessary measures to properly protect personal data.

187 https://ec.europa.eu/home-affairs/policies/schengen-borders-and-visa/visa-policy_en, under 'Statistics on short-stay visas issued by the Schengen States', last accessed 23 February 2022.

225. The AP also takes into consideration that BZ has already identified risks in its own analyzes (from 2015 and 2020). area of information security related to NVIS and not timely and/or has taken insufficient action.188 For example, BZ has assessed the risk in 2015 and in 2020 defined that power failures can cause equipment to malfunction and that unauthorized persons be able to make changes in NVIS as a result of insufficient governance with regard to authorizations. the AP also points on this point to the Accountability Investigations by the Court of Audit in 2017, 2018 and 2019, from which it follows that the deficiencies in information security for BZ also apply to were already known. The Court of Audit has established that BZ runs risks on the focus areas governance, organizational structure and risk management. Also has the Court of Audit has ruled that BZ does not have a management framework to regulate the implementation and implementation of

to properly initiate and control information security within the organization.

226. In view of the above, the AP sees, on the basis of Article 7, opening words and under b, of the Fine Policy Rules reason to increase the fine even further, to an amount of € 440,000.

3.3.3 Categories of personal data

227. The AP has established that, in the context of processing applications for Schengen visas, BZ special personal data, such as fingerprints. Such data qualifies as biometric data. Even higher protection is required for special personal data. the AP has established that the Ministry of Foreign Affairs does not adequately assess the risk for a very large group of those involved appropriate security level for this category of special personal data.

228. In view of the above, the AP sees, on the basis of Article 7, opening words and under g, of the Fine Policy Rules reason to increase the fine to € 465,000.

3.4 Fine for violation of the provision of information to data subjects

229. The controller should provide the data subject with information necessary to to ensure fair and transparent processing vis-à-vis the data subject, taking into account of the specific circumstances and context in which the personal data are processed.189 The AP has established that the Ministry of Foreign Affairs does not report in the context of the provision of information to visa applicants makes the sharing of personal data with third private parties and thus Article 13(1)(e) GDPR violates.

230. As mentioned above, BZ processes a lot of (special) personal data. It must be for those involved be transparent with which (categories of) recipients BZ shares this personal data. Considering the species personal data, the fact that hundreds of thousands of data subjects are insufficiently informed and the violation has lasted for 3.5 years and is still continuing, the AP considers the imposition of an administrative fine appropriate.

188 File 3, appendix 5a: Vulnerability analysis and DCV IS plan; Written Opinion BZ dated 15 October 2021, appendix 3.

189 See Recital 60 of the GDPR.

231. With regard to the amount of the fine, the AP considers that the consequences of this violation

232.

are limited. This means that, from a proportionality point of view, the AP sees reason to set the basic amount of the fine from €525,000 to €100,000.

3.5 Blame and proportionality for both violations

Pursuant to Article 5:46, second paragraph, of the Awb, when imposing an administrative fine, the AP into account the extent to which this can be blamed on the offender. Now that this is a violation, the imposition of an administrative fine in accordance with established case law does not require that it is demonstrated that there is intent and the AP may presume culpability if it offense is established.

233. BZ is obliged to carry out a risk assessment by means of appropriate technical and organizational measures appropriate security level. In addition, BZ must make it sufficiently clear to those involved determine to which parties it provides personal data. BZ is to blame for not doing this fulfills two obligations. The AVG, but also the VIS Regulation and BIO with which BZ must comply, have explicitly described with regard to the security of the processing of personal data organizations must maintain a risk-adjusted level of security. Furthermore, the GDPR (and the guidelines on transparency) provide sufficient explanation as to what information is stakeholders should be shared. BZ may be expected to comply with the applicable standards and act accordingly.

234.

Finally, pursuant to Articles 3:4 and 5:46 of the Awb, the AP assesses whether the application of its policy for

determining the amount of the fines in view of the circumstances of the specific case, not to a

disproportionate outcome.

235. The AP is of the opinion that (the amount of) both fines is proportional.190 In this opinion, the AP has

others have taken into account the seriousness of the infringements and the extent to which they can be blamed on BZ.

Due to the nature of the personal data, the duration of the violations, the fact that the violations

have not yet been terminated and the risks that data subjects run, the AP qualifies the relevant

breaches of the GDPR as serious. With regard to the amount of the fine for the violation of the

information provision to those involved, the AP has already substantiated in paragraph 3.4 why the

the fine determined is proportionate in its opinion.

236. In view of the foregoing, the AP sees no reason to set the amount of both fines under the

proportionality and the circumstances mentioned in the Fines Policy Rules, to the extent applicable in the

present case, further increase or decrease.

3.6 Conclusion

237. The AP sets the total fine at € 565,000.

190 For the justification, see also paragraphs 3.3 and 3.4.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

4. Order subject to penalty

238. Now that it is a continuous violation of Article 32(1) GDPR and Article 13(1)(e) GDPR

BZ must end these violations as soon as possible. For that reason, the AP explains on the basis of

Article 58, paragraph 2, preamble and under d, GDPR jo. article 16, paragraph 1, UAVG and article 5:32, paragraph 1, Awb to

the

Minister also ordered a cease and desist order.

239. The AP orders the Minister of Foreign Affairs in the context of handling applications from Schengen visa:

1. to end the violation of Article 32(1) of the GDPR by appropriate technical and organizational take measures to ensure a level of security appropriate to the risk.

To this end, the Minister serves the national information system for the purpose of processing from Schengen visas:

a. to draw up an information security policy that also states how BZ applies this policy periodically review and adjust if necessary.

b. prepare emergency plans and protect equipment against disruptions in utilities.

c. take adequate safeguards for physical security when working in this national system in public areas.

d. to establish how BZ ensures regular checks on access rights to this system.

This also means that access rights must be checked regularly and be adjusted without delay if an audit shows that an employee is wrongly authorized to have access to personal data.

e. ensure that it is possible to verify and establish which data, when, by who are processed and for what purpose.

f. to record how BZ logging and the regular checks on this in this system guarantees. This also means that BZ must regularly check log files.

It is up to the Minister, as the controller, to determine the exact interpretation of the to determine the above remedial measures.

2. to end the violation of Article 13(1)(e) GDPR.

The Minister should achieve this by providing information about the recipients or categories of recipients of the personal data to data subjects (when obtaining the personal data).

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

Beneficiary term and amount of penalty with regard to part 1

240. The AP attaches to part 1 of this charge a beneficiary period that ends on October 24, 2022.

241.

If the Minister for Foreign Affairs does not comply with the order before the end of this beneficiary period,

complies, he forfeits a penalty. The AP sets the amount of this penalty at an amount of

€ 50,000 for every two weeks after the end of the last day of the set term on which the Minister

of the Ministry of Foreign Affairs fails to comply with part 1 of the order, up to a maximum of

€500,000.

Beneficiary term and amount of penalty with regard to part 2

242. With regard to part 2 of this burden, the AP is of the opinion that with its implementation less

243.

efforts are involved. The AP therefore attaches to part 2 a beneficiary period that ends

March 24, 2022.

If the Minister for Foreign Affairs does not comply with the order before the end of this beneficiary period,

complies, he forfeits a penalty. The AP sets the amount of this penalty at an amount of

€10,000 for each (entire) week, after the last day of the set term, on which the

Minister of Foreign Affairs fails to comply with part 2 of the order, up to a maximum of

€300,000.

244. In the opinion of the AP, the amount of the above amounts for both parts of the burden

in reasonable proportion to the gravity of the interests violated by the violations, namely the

protection of (special) personal data and transparency about the processing to

involved. The AP also finds the amounts sufficiently high to induce BZ to commit the violation

to end.

245. The above measures are within the power of the Ministry of Foreign Affairs to take and the timeframe to implement these

measures

to take deems the AP realistic. In doing so, the AP has taken into account that a large part of the

measures that BZ must take in part 1 primarily comprises the preparation of documentation. And for

with regard to part 2, BZ only needs to adjust the information provision to a small extent.

Follow-up

If BZ wishes to forfeit penalty payments immediately after the end of the beneficiary period,

occur, the AP recommends BZ to submit the documents – with which BZ can demonstrate that it complies

to the order – on time, but no later than one week before the end of the beneficiary period to the AP ter

to send a review.

246.

247. Finally, the AP advises BZ to regularly communicate on the basis of a concrete planning

inform the AP about the progress of the measures it is taking to comply with part 1

of the imposed burden.

5. Operative part

The AP has come to the conclusion that the Minister of Foreign Affairs, if

controller in the process of granting Schengen visas, data subjects

insufficiently informs and the security of the processing of personal data insufficient

guarantees. In view of the fact that the Minister of Foreign Affairs contains a great deal of (sensitive) personal data

processed from hundreds of thousands of data subjects and the violations still persist after 3.5 years,

the AP qualifies the relevant violations of the GDPR as serious.

That is why the AP imposes an administrative fine on the Minister of Foreign Affairs and also

a burden under duress.

- The AP submits to the Minister of Foreign Affairs for violation of Article 32(1) of the GDPR

and Article 13, paragraph 1 under e, GDPR, an administrative fine amounting to: € 565,000 (in words:

five hundred and sixty-five thousand euros).191

- The AP orders the Minister of Foreign Affairs in the context of handling applications

from Schengen visas:

1. take appropriate technical and organizational measures to ensure a risk-adjusted

to ensure a level of security and thus to prevent the violation of Article 32(1) of the GDPR

to end; and

2. information about the recipients or categories of recipients of the personal data to

data subjects (when obtaining the personal data) and thus the

to end the violation of Article 13(1)(e) GDPR.

If the Minister of Foreign Affairs with regard to part 1 does not comply with the

fulfills the burden, he forfeits a penalty. The AP sets the amount of this penalty at an amount of

€50,000 (in words: fifty thousand euros) for every two weeks after the end of the last day of the

term within which the Minister of Foreign Affairs fails to comply with part 1 of the order, up to a

maximum of €500,000 (in words: five hundred thousand euros).

If the Minister for Foreign Affairs does not comply with the

fulfills the burden, he forfeits a penalty. The AP sets the amount of this penalty at an amount of

€ 10,000 (in words: ten thousand euros) for each (entire) week, after the end of the last day of the

term, on which the Minister of Foreign Affairs fails to comply with part 2 of the order, up to a

maximum of € 300,000 (in words: three hundred thousand euros).

191 The AP will hand over the aforementioned claim to the Central Judicial Collection Agency (CJIB). The fine must be in

accordance with

Article 4:87(1) Awb to be paid within six weeks. For information and/or instruction about payment, please contact

be recorded with the aforementioned contact person at the AP.

59/64

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

Yours faithfully,

Authority Personal Data,

w.g.

ir. M.J. Verdier

Vice President

Remedies Clause

If you do not agree with this decision, you can return it within six weeks of the date of dispatch of the

decide to submit a notice of objection digitally or on paper to the Dutch Data Protection Authority. In accordance with

Article 38 of the UAVG suspends the effect of the decision to lodge a notice of objection

imposition of the administrative fine. Submitting a notice of objection suspends the effect of the order

subject to periodic penalty payments in this decision. For submitting a digital objection, see

www.autoriteitpersoonsgegevens.nl, under the heading Objecting to a decision, at the bottom of the

page under the heading Contact with the Dutch Data Protection Authority. The address for paper submission

is: Dutch Data Protection Authority, PO Box 93374, 2509 AJ The Hague. Please state 'Awb objection' on the envelope

and put 'objection' in the title of your letter. In your notice of objection, write at least:

- your name and address;

- the date of your notice of objection;

- the reference mentioned in this letter (case number); or attach a copy of this decision;

- the reason(s) why you do not agree with this decision;

- your signature.

60/64

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

ATTACHMENT 1

The following legislation forms the basis of the legal framework for this Decree:

 The General Data Protection Regulation (GDPR) sets the general legal framework

for the processing of personal data, and the supervision of the AP.

 The Regulation on the Visa Information System (VIS) and the exchange between the

Member States of data in the field of short-stay visas (hereinafter: VIS Regulation192) gives

the specific frameworks with regard to the European Visa Information System that the member states

use for mutual cooperation in the issuance of visas. This regulation regulates

including which bodies are responsible for data processing through the VIS. The

VIS Regulation prescribes which data of data subjects who have a visa for the

Schengen area applications must be included in the (national)

visa information system.193

The VIS Regulation also describes, among other things, the purpose and functions of VIS and sets requirements for

the parties responsible for the use of the VIS.194 This includes:

safeguards for the integrity and confidentiality of visa information.195

 The Regulation establishing a Community Code on Visas (hereinafter: Visa Code)196

outlines the general framework that Member States must comply with in the context of the application and

issuance of visas.197 This framework determines, among other things, which data must be processed for the purpose of

applying for and issuing a visa for the Schengen area and various preconditions

with which the Member States must comply in this process.

The AP has assessed against the following provisions:

Explanation

The GDPR contains the general legal framework for the processing of personal data. The for this decision

relevant standards from the GDPR are:

Definitions

Article 4 GDPR defines a number of basic concepts from data protection law that are used in this decision

have been applied. Specifically addressed is the concept of “personal data”, the processing of

personal data, the controller and the processor.198

192 Retrieval: https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=celex%3A32008R0767

193 See Article 9 of the VIS Regulation

194 See, for example, Articles 1 and 47 VIS Regulation

195 See, for example, Articles 1 and 28 VIS Regulation

196 Retrieval: https://eur-lex.europa.eu/legal-content/NL/ALL/?uri=CELEX%3A32009R0810

197 Article 1 Visa code: This Regulation establishes the procedures and conditions for issuing visas for transit through the

territory of the Member States or an intended stay in the territory of the Member States not exceeding three months within a

period

of six months.

198 Article 4, parts 1, 2, 7 and 8.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

Principles

Article 5 GDPR describes a number of basic principles that must generally be complied with in order to

process personal data in accordance with the Regulation. In particular the principles
transparency, integrity and confidentiality play a role in this case. These principles from article 5 paragraph 1,
under a and under f of the GDPR are further specified by the more specific provisions in the GDPR and, in the
context of the present Decree, in the specific legal framework relating to
visa information systems.

Processing security

Article 32 GDPR prescribes – in short – that the controller and the processor
must take appropriate technical and organizational measures to ensure a risk-adjusted
to ensure a level of security. The general standard for securing
personal data in Article 32 GDPR means that the controller, taking into account
the state of the art, the implementation costs, as well as the nature, scope, context and
processing purposes and the risks of varying likelihood and severity to the rights and
freedoms of persons, must take appropriate technical and organizational measures to
risk-adjusted security level.

The term 'appropriate' also indicates a proportionality between security measures and the nature of
the data to be protected. The more sensitive data is, or the context in which it is
are used represent a greater threat to privacy, become more serious
requirements for the security of this data.199

To further determine which security measures are appropriate, apply in most sectors
more specific standards for information security. Most relevant security standards for the
government are contained in De Baseline Information Security Government (BIO).200 The BIO is completely
structured according to NEN-ISO/IEC 27001:2017, Annex A and NEN-ISO/IEC 27002:2017. The forum
Standardization has included these standards in the 'comply-or-explain' list of mandatory standards
for the public sector, according to the comply or explain principle. This means that the government must comply with these
standards
unless there are explicitly stated reasons not to do so.

The AP notes in this regard that the Government Baseline Information Security has been in effect since January 1, 2020. various baselines and standards from various public sectors have been united into an overarching standard for the entire government. At the start of the study in 2019, the relevant security aspects further elaborated in the Baseline Information Security Central Government Service (hereinafter: BIR). The BIR is also based on the ISO 27002 standards and valid until the end of 2019.

The AP has reviewed the state of data processing security through the national Visa Information System also specifically assessed against Article 32(2) of the VIS Regulation. This article looks at the taking security measures, including a security plan. These provisions from the VIS

199 Dutch Data Protection Authority: Policy rules on the security of personal data, February 2013 3, p. 1 0 and Parliamentary Papers II 1 997-1 998, 25 892, no. 3, pg. 99.

200 For the government, the Government Baseline Information Security (BIO) is the leading standard. In this case, its predecessor is also the BIR is important because the BIR was the standard at the start of the study until the end of 2019. Both standards are based on the ISO27000 standards in the field of information security.

Regulation forms a lex specialis, of what is described in Article 32 GDPR as 'appropriate' measures'.

In view of the scope of the present decision, the AP has considered the following aspects of this article: tested:

- Article 32, paragraph 2, VIS Regulation first of all prescribes that there must be a security plan to

the confidentiality and integrity of data processing through NVIS

guarantees.

- Member States should take measures to physically protect data, including

drawing up emergency plans for the protection of critical infrastructure, according to article 32 paragraph 2

under a, VIS Regulation.

- According to Article 32(2)(f) of the VIS Regulation, Member States must take measures to

ensure that those authorized to consult the VIS only have access

to the data to which their access authorization relates, and only with

personal and unique user identities and secret access procedures (control of the

access to the data) This means that there must be an appropriate authorization policy for the

access to NVIS and that the roles assigned in that context must be managed.

- To monitor in the organization which persons may be eligible for authorizations

for the use of NVIS, Article 32(2)(g) of the VIS Regulation provides as additional safeguard

that all authorities with a right of access to the VIS draw up personnel profiles in which the tasks

and responsibilities are described of the persons authorized to

to view, record, update, delete and search. These profiles must

can be made available to the DPA upon request and without delay.

- Article 32, second paragraph, under i, of the VIS Regulation prescribes that each Member State with regard to

-

its national system, adopts the necessary measures to ensure that it is possible to

verify and determine which data is in the VIS when, by whom and for what purpose

incorporated. That means that BZ has to keep log files.

Article 32, second paragraph, under k of the VIS Regulation provides that the efficiency of the

security measures is checked and with regard to this internal control the

necessary organizational measures are taken to ensure that the regulations

of this regulation are complied with (checking the log files). This also includes the

security regulations of Article 32 GDPR.

Integrity in Visa Information Processing

Article 28(5) VIS Regulation requires that personnel wishing to process data contained in the VIS stored, first receive proper training on the rules of data security and protection. Only after this training has been received can personnel be allowed to enter the VIS process stored data. This article can be seen as a concrete elaboration of the principle of integrity, which is laid down in Article 5(1)(f) GDPR. Based on this principle, a controller implement organizational safeguards that ensure integrity and confidentiality of data processing.

Providing information to the data subject

Being transparent about data processing is, as mentioned above, one of the general principles for proper data processing. Informing the data subject about a

data processing contributes to transparency. In this context, Article 13 GDPR and in particular Article 37 VIS Regulation relevant. Article 37 VIS Regulation constitutes a specification of what is laid down in Article 13 GDPR. The AP has checked whether at the start of the procedure for applying for a Schengen visa, the obligation to provide adequate information about it to the person applying for a visa.

This produces the following picture of relevant standards, arranged from general to specific for the visa process.

Figure 1: Schematic representation of the legal framework:

Special □

Data security

NVIS:

Art. 32 paragraph 2 VIS Vo

Security plan:

Art 32 paragraph 2 preamble VIS Vo

BIO version 1.0.4, part 2, chapter 5

(p. 27):

standards under section 5.1.

General

Confidentiality and

integrity of

data processing

Art 5 para. 1(f) GDPR

Art 24 GDPR

Art. 32 GDPR

Physical security:

Art 32 paragraph 2 sub a VIS Vo

Access rights and

personnel profiles

Art 6 paragraph 1 VIS Vo

Art 32 paragraph 2 sub f and k jo

FISH Vo

Art Art 32 paragraph 2 sub g VIS

fo.

Logging (internal

check):

Art 32 paragraph 2 sub f, i and k

VIS Vo.

Security Incidents

(internal control):

Art 32 paragraph 2 sub c, d and k

VIS Vo.

BIO version 1.0.4, part 2, chapter

11 (p. 43):

standards under section 11.1 and

11.2.

BIO version 1.0.4, part 2, chapter 9

(p. 37):

standards under section 9.2.

BIO version 1.0.4, part 2, chapter

12 (p. 50):

standards under section 12.4.

BIO version 1.0.4, part 2, chapter

16 (p. 63):

standards under section 16.1.

64/64

Art. 5 paragraph 1(f) (guarantee

in the organization on

area of integrity and

confidentiality)

Information to

involved

Art. 5 para. 1(a) GDPR

Art. 13 GDPR

Staff training

regarding

data protection:

Art 28 paragraph 5 Vis Vo

Art 38 paragraph 3 Visa code.

Right to information:

Art. 37 VIS Vo.