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

authoritypersonal 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]

Subject

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 relates

until the New Visa Information System (NVIS) established in short that:

there is no security plan;

insufficient measures have been taken to physically protect personal data;

-

-

- incomplete procedures exist regarding (the 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 contrary to Article 13, paragraph 1 under e, and Article 32, paragraph 1, of the General Data Protection Regulation (GDPR). The AP has also decided to issue you with an order subject to periodic penalty payments to impose, which sees to the undoing of these transgressions – which in establishing 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. The (amount of the) administrative fine is elaborated in chapter 3 and is stated in chapter 4 described the order subject to periodic penalty payments. Finally, Chapter 5 contains the operative part and the legal remedies clause.

Contents

19

19

22

25

25

26

32

36

36

37

40

42

42

44

47

48

48

48

49

50

51

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

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 ones
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 is through a national system, te
know: N.VIS. The specific application that is under N.VIS and by the Ministry of Foreign Affairs
(hereinafter: BZ) is used for Schengen visas, is the New Visa Information System
(hereinafter: NVIS).

The NVIS contains the application data, including biometric data, of all applicants who have submitted via a
Dutch consular post abroad want to obtain Schengen visas for 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
During the processing of visa applications, it is also always checked whether the applicant is included in SIS II. SIS
II includes alerts introduced by member states in the field of European arrest warrants and, among other things

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 of the national part of SIS II and VIS was assessed. The Schengen evaluation report 2015 is explicit stipulates that the AP must carry out regular checks at the Dutch consular posts. This AP checks are also part of the police and judiciary multi-year plan that the AP follows in the framework of its supervision of, among others, the aforementioned SIS II and VIS (systems).

In response to this, the AP has conducted an audit at BZ and a number of parties who have a role in the process of issuing Schengen visas. The research included the following organizations:

- the Dutch embassy in London, United Kingdom (hereinafter: London consular post);
- 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
-
-
-

granting a visa (hereinafter: the CSO);

[CONFIDENTIAL] (hereinafter: Processor 1) in London, United Kingdom, which acts as external service provider (hereinafter: EDV) in the visa process of the London Consular Post;

[CONFIDENTIAL] (hereinafter: Processor 2) in Utrecht, the performer of various IT tasks in relationship 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 research 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, the physical security, the granting of access rights to NVIS and the logging of it NVIS usage. In addition, compliance with the legal requirements was checked with regard to the provision of information to visa applicants and the training of employees involved in it 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 London and Dublin consular posts.

5.

6.

Short stay Schengen visa

A short stay visa is called a 'Schengen visa'. This visa allows individuals to enter a period of 180 days, stay 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 case of a positive decision

the visa sticker is printed and pasted in the applicant's passport, in the event of a negative decision

made a refusal decision. In both cases, the decision is registered in VIS.5

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

2 When processing visa applications, it is 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 area 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 document 3, appendix 3: Visio-Schengen Flowchart, p. 6 and 7.

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

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

Date

[CONFIDENTIAL]

9.

10.

11.

12.

Apply for a Schengen visa at the London consular post

The London Consular Post works together with Processor 1, which fulfills the 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 from the Ministry of Foreign Affairs website or via the website of Processor 1. The applicant then makes an appointment with Processor 1 via the Processor 1 appointment system. On the day of the appointment, the applicant reports to Processor 1.

Processor 1 successively performs the following tasks:8

[CONFIDENTIAL]

The London Consular Post carries out the following tasks, among others:

[CONFIDENTIAL]

The tasks of the CSO include the following activities:9

[CONFIDENTIAL]

6 Recital 13 Visa Code, Article 40 paragraph 3 Visa Code, Article 43 Visa Code.

7 Article 43(5) Visa Code.

8 File document 3, appendix 3: Visio-Schengen visa Flowchart.

9 File document 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) is necessary or is it necessary to consult or inform Member States.10 In addition, it is possible

necessary to interview the applicant.11 During the processing of visa applications

always checked whether the applicant is in SIS II. The SIS II check takes place automatically, in the

background of a visa application through 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 case of a positive decision

the visa sticker is printed and pasted in the applicant's passport, in the event of a negative decision

issued a refusal order. In both cases, the decision is registered in VIS.13

Apply for a Schengen visa at the Dublin consular post

During the AP's investigation, the Dublin Consular Post operated without the intervention of an EDV and

processes visa applications itself. This largely uses the same steps of the

visa application process followed as 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 Ministry of Foreign Affairs. An appointment for an intake at the consulate can be made

on the website of the embassy via a link to an appointment system.

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

[CONFIDENTIAL]

In its role as back office, the CSO performs the same tasks as those of the consular post

London. In addition, the CSO has an important task in registering the visa application data

which occupies the Dublin consular post and as paper files by post to the CSO in The Hague

sends.

BZ 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 now takes live photos and the intake of the visa applications

no longer takes place by post (through the London consular post). In addition, consular mail makes Dublin

now using an EDV.14

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

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

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

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

14 Written View of the Ministry of Foreign Affairs of 15 October 2021, p 3.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

18.

19.

20.

1.4 Legal framework

The AP refers to APPENDIX 1 for the legal framework.

1.5 Process flow

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

desk investigation, requested information in writing and has several

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

conducted interviews and researched the information systems used in the

visa process. Following the OTPs performed, the AP has the additional documentation

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

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

databases (particularly tables of the databases).

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

On October 15, 2021, the Minister gave a written opinion on this intention and the associated measures

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

opinion hearing was held at which BZ also explained its opinion orally.16 On 10

In December 2021, BZ sent further documents on request.17

15 Written View of the Ministry of Foreign Affairs of 15 October 2021.

16 Letter from BZ 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 Factual findings

The Visa Code specifies which data the Member States must collect in order to be able to issue visas
provide. The VIS Regulation stipulates that the following data for the
handling and taking decisions on visa applications for the Schengen area in the VIS
must 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 immediately retrieves the application file by entering various data in the VIS,
such as the first and last name, gender, place and country of birth, nationality, type of visa that will be
applied for, purpose of the trip, place of residence, current profession, photograph and fingerprints of the applicant.19
Authorized staff of the visa authorities can access and use the VIS
entering, changing or deleting data.20 For example, when a visa is issued, when a
a visa application, in the event of a refusal of a visa application, in the event of an annulment/withdrawal of a
visa or a visa extension21 data added to the application file. Next 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 is stored for the benefit of the
Schengen visa process are saved, modified and deleted.

2.1.2 Legal Review

The data of visa applicants processed in the NVIS qualify as personal data in the sense
of Article 4(1) GDPR, because it concerns information about identified natural persons.23 A
part of this data is biometric data within the meaning of Article 4, under 14, and Article 9 GDPR
and therefore 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) GDPR. The AP
notes that personal data is processed by means of the NVIS when going through it
visa process for short term stay.

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 data between Member States in the field of short-stay visas ('VIS Regulation'), OJ 2008, L218/60.

19 Article 8(1) in conjunction. 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 BSN are processed, the identity of the persons is established and it 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 notes that the Minister of Foreign Affairs is the designated responsible person for the Netherlands processing of personal data in the VIS.24

The AP notes 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

includes a number of directorates, two of which play a particular role in the granting of visas.

Firstly, the Consular Affairs and Visa Policy Directorate (DCV). DCV is responsible for, among other things providing consular services to Dutch nationals abroad and managing the consular function in the department and at the posts.26Second, 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 granting of visas and travel documents. The AP has confirmed, and BZ has confirmed, that the back office of the consulate London and the consulate Dublin located at CSO. In addition, CSO takes care of the back office activities with regard to a number of companies other consular services and products.27

Processor 1

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

Processor 1 has been designated as an external service provider28 to facilitate visa application facilities. It company is setting up physical visitor centers where those involved can submit their applications. In London Processor 1 provides the front office for BZ for 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 data received from the applicant. At the location of [CONFIDENTIAL] in London, ICT facilities installed [CONFIDENTIAL].30 Processor 1 has no 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, change, delete or consult data (2012/C79/05).

25 Article 7, paragraph 2, sub d, Foreign Affairs Organization Decree 2019.

26 Article 7, paragraph 2, sub c, Foreign Affairs Organization Decree 2019.

27 Article 7, paragraph 2, sub d, Foreign Affairs Organization Decree 2019.

28 Article 40(3) Visa Code.

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

30 File document 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 rules set by the European Commission, in accordance with Article 46(2)(c) GDPR established standard contractual clauses on data protection (“Standard Contractual

Clauses´).31 In Article 1, under b and c, the following is laid down:

(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, sub b, Standard Contractual Clauses, the 'data exporter' commits itself the obligation 'that it has been 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'.

In appendix 1 to the Standard Contractual Clauses it is stated that BZ is the 'data exporter' and [CONFIDENTIAL] the 'data importer'.32

Processor 2

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

The services for 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 concluded an agreement with BZ on 31 August 2010 for the supply of support services for NVIS. The service includes 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 simplify the visa issuing process support.34 Processor 2 reports to the Director of Consular Affairs and Visa Policy of Foreign Affairs.35

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

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

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

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

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

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

11/64

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

36.

37.

38.

39.

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

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 is sub-

processors can engage for the processing of personal data when there is

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

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

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

Processing Agreement.

Article 5.1 of the processing agreement between BZ and Processor 2 states that BZ has the right

to be audited once per contract year by a certified internal or external auditor

to Processor 2's compliance with its obligations under the Processor Agreement. The AP

has determined that BZ evaluates the compliance of Processor 2 by requiring so-called

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

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

The DPA has determined that Processor 2, in the context of its services for NVIS, uses the

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

manages data storage centers worldwide. Processor 3 has a data center in the Netherlands 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 Review

Controller

In accordance with the VIS Regulation (Article 41(4)), each Member State shall designate for the processing of personal data in the VIS indicates the authority that should be regarded 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 document 14, appendix 02.1: GDPR Amendment Agreement Processor 2 – Min BZ NVIS 20180529.

37 File document 14, appendix 12.2: [CONFIDENTIAL].

38 File document 20: [CONFIDENTIAL].

39 File document 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 will be processed

to be processed and also takes 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, in the sense of

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

this decision is called BZ, the AP equates this with the Minister of Foreign Affairs.

Processors

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

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

into a legal instrument with the minimum requirements set out in the Visa Code.42

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

namely Processor 1 (the external service provider that processes the visa applications

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

provides support to Processor 2's processes. Be there 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

said parties as processors.

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

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

paragraph 2 and paragraph 4 GDPR (sub-processor).

2.3 Security plan NVIS

2.3.1 Legal framework

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

establishes security measures, including a security plan. This plan is one of them

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

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

more generally, that the responsible measures in the field of compliance with the

GDPR and that they must be periodically evaluated.

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 document 12, appendix 44a: pia application station signed and file document 12, appendix 44b: nvis pia

signed.

42 Annex X Visa Code.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

preconditions that BZ applies for information security in relation to NVIS must be made clear

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 referred to in Article 32, paragraph

2, VIS Regulation are included.

The Baseline Information Security Government (BIO) also prescribes 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 the purpose of information security, a set of policies should be established

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

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

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

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

security policy and 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

line managers.

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

apply.

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

f. The promotion of security awareness.

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

governance and P&C cycles and external developments assessed and adjusted where necessary.

2.3.2 Factual findings

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

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

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

London and Dublin. The AP has also requested written documentation relating to the

existence and content of a security plan.

Ministry of Foreign Affairs

The AP has established that during the investigation, BZ submitted an (N)VIS to the AP43's request for a security plan provide, replied with three documents, namely:

48.

49.

- Vulnerability analysis and IS plan DCV44

- PIA Request Station45

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

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

45 File document 3, appendix 5b: PIA Request Station.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

- Quick scan Schengen visa February 201946

50.

51.

52.

53.

54.

The January 2015 “Vulnerability Analysis and IB Plan DCV” contains a risk assessment, with regard to to DCV's business processes for granting visas and the posts left by DCV's management to comply with the obligations of the Information Security Regulations Decree Rijksdienst 2007. The report includes a report on the relevant threats and

vulnerabilities of information systems. The report also contains measures that have been adopted
risks to an acceptable level. The report qualifies these proposed measures
as an “information security plan” including prioritization.
The “PIA Requesting Station” is a Privacy Impact Assessment of the requesting station. It
The end result of the PIA is a set of risks and recommendations for the security measures to be taken
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 imposed by the business processes on the Schengen visa process
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 into
whether these requirements fall within the Baseline information security or whether they exceed 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 ordered in the QuickScan.
Based on these three documents, the AP notes that BZ has a number of different documents,
in which (proposed) security measures are mentioned. Some of those measures
directly related to NVIS.
Consular Post London
During the on-site investigation on July 2, 2019 in London, the AP requested for completeness
access to the security plan regarding NVIS. The London Consular Post has one
standard format security plan supplied by Foreign Affairs and locally used by the consular post
entered. Two inspectors from the AP and the FG from BZ have had access to the most recent version
of the security plan. [CONFIDENTIAL]:
[CONFIDENTIAL]
The said documents relate to the security of the London Consular Post, in particular
[CONFIDENTIAL], and are not aimed at the information security of NVIS and the visa process. The AP
notes that it has seen documentation at the consular post in London that does not pertain to the

information security related to NVIS.47

46 File document 3, appendix 5c: Quick scan Schengen visa February 2019.

47 File document 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 has also checked in Dublin whether there is a security plan regarding NVIS in practice
was available. During the on-site investigation on January 22, 2020 at the consular post in Dublin
stated that a security plan is in place. It is a standard format security plan that is used by
BZ is delivered and completed locally at the post office. An adjustment of the security plan will be
done once a year by the deputy chief of post.48

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

[CONFIDENTIAL].50

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

CSO The Hague

The AP has checked with CSO whether a security plan in the sense 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 report – [CONFIDENTIAL];56

- Security analysis stolen secure mail CSO;57

- Security analysis building burglary;58

- Security analysis intrusion mer and ser;59

- Security example Unauthorized [CONFIDENTIAL];60

- Security example info in the event of an unexpected visit;61

48 File document 27: Report of official acts consular post Dublin.

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

50 On site, the AP inspectors established that inspection of this document was not necessary for the investigation.

51 File document 27: Report of official acts consular post Dublin.

52 File document 13: AP information request dated 25 July 2019.

53 File document 14: Response of the Ministry of Foreign Affairs of 8 August 2019 to Information AP of 25 July 2019.

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

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

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

57 File document 14, appendix 16.3: Security analysis stolen secured mail CSO.

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

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

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

61 File document 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

are not specifically directed at or related to NVIS. There are also no concrete references to it

visa process encountered.

2.3.3 Legal Review

The AP notes 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 were brought forward at or following AP's visit

to CSO.

60. With regard to the documents submitted, the AP establishes the following.

The “Vulnerability analysis and IB plan DCV” contains a number of security measures, but is not

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

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

accompanying the

CSO are requested, are not specifically aimed at NVIS and only refer to a limited number

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

are prescribed. The measures in these documents mainly concern 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(2)(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 set any requirements for the form

of a security plan and also does not require a security plan solely on the national visa

information system. BZ considers a number of documents in conjunction as a security plan

for NVIS63:

- Privacy Impact Assessment Schengen and Caribbean Visa of October 25, 2018.

- Baseline test NVIS

- Quick scan Schengen visa February 2019 and the Risk analysis 'Vulnerability analysis and IB plan

DCV'.

BZ has stated in its opinion that BZ regrets to have found that the earlier

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 DPA, has assessed in the context of the VIS audit that BZ has

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. During the investigation, the AP at various times

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 processes that did not take place simultaneously. The VIS audit was

61.

62.

63.

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

63 Written View of the Ministry of Foreign Affairs of 15 October 2021, p. 4.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

64.

65.

66.

67.

broader in scope and used a different assessment framework. In addition, the external auditor only established that 1) not him but BZ the combination of the Baseline test, PIA and risk analysis together regarded as 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 constitute a plan aimed at information security its whole. The submitted 'Baseline test NVIS' is a kind of completed questionnaire/checklist. It is a enumeration of BIO standards with commands for making and taking security measures, whereby it is not clear to the AP how the answers should be given be indicated. Based on these documents, it is unclear to the AP which policy measures and specific control measures BZ has taken 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 the Ministry of Foreign Affairs to have a security plan drawn up for NVIS, in which at least attention is paid to points a to k from article 32(2) VIS Regulation. In the AP's opinion, BZ has insufficiently demonstrated this. BZ has for example, a security plan has not been submitted that states 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 the Ministry of Foreign Affairs that describes how and when BZ performs checks on logging. The general procedure of BZ at the time of the investigation provided for reporting security incidents by BZ employees was not sufficient. And the procedures for granting and checking access rights to the NVIS environment have only been introduced by BZ

adopted in January 2022. The AP refers to sections 2.4, 2.5, 2.6 and 2.7 for the detailed assessment of these procedures. The AP concludes that the documents presented by BZ as - in their entirety reviewed - an information security plan does not meet the preconditions to be set.

In view of the BIO standards, the AP further notes that due to the lack of (essential parts in) information security policy, do not update this policy at scheduled intervals (or if significant changes) has been assessed by BZ to ensure that it continues to be appropriate, adequate and effective. Securing information is a process that always involves a Plan-Do-Check-Act cycle must be completed, as laid down in 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 notes that BZ in the 'Baseline information security BZ 2021' is at a high level of abstraction has established who for implementation and implementation of BIO standards is responsible. The Personal Data Protection Policy describes the PDCA cycle with regard to the protection of personal data, but does not contain the security aspects thereof. The same applies to the Grip on privacy document, the AVG manual, in control statements and the follow-up memo submitted. BZ has published risk analyzes from 2015 and 2020 and a plan of measures

64 Written View of the Ministry of Foreign Affairs of 15 October 2021, p. 4.

68.

69.

November 2021 show that it only occasionally has security measures related to NVIS evaluated and acted upon.

Based on the above, the DPA concludes that BZ has no security plan (and therefore this

has also not evaluated) that meets the requirements of Articles 24 and 32 (1) GDPR and further elaborated in Article 32(2), introductory phrase, 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) 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 the points at which physical security can be checked become. The BIO does not literally describe goals that must be achieved (the “what”) how 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 control ensure that only authorized personnel are allowed access.

Securing offices, spaces and facilities

For offices, rooms and facilities, physical security should be designed and

applied.

Protect against outside threats

Physical protection is required against natural disasters, malicious attacks or accidents

to be designed and applied.

Working in secure areas

Procedures should be developed and implemented for working in secure areas

applied.

Utilities

Equipment should be protected against power failures and other disturbances

caused by disruptions in utilities.

2.4.2 Factual findings

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

Hague, Processor 2 in Utrecht and Processor 3 in Amsterdam. The AP has per location during the checks

70.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

71.

72.

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

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

NVIS environment is possible and/or whether the intake process for Schengen visas takes place.65 Per

location described the situation found during the on-site investigations.

Consular Post London

[CONFIDENTIAL]66

Processor 1 London

[CONFIDENTIAL] 67

65 [CONFIDENTIAL]

66 File document 7: Report of official acts OTP consular post London.

67 File document 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 Document 27: Report of Official Acts OTP Consular Post Dublin.

69 File document 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 Review

The AP first of all notes that measures have been taken in the area of

physical security. The AP concludes that measures have been taken to protect the buildings and the space(s)

in which data of visa applicants are processed, including with cameras

and motion sensors. The AP also concludes that the areas in which personal data of

visa applicants are processed as secured zones.

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

71 File document 20: [CONFIDENTIAL]

72 File document 21: Email Ministry of Foreign Affairs of 13 November 2019 with documents in response to OTP 8 November.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

78.

79.

80.

81.

82.

However, the AP notes that BZ has not explicitly determined which parts of the IT infrastructure

should be regarded as the critical infrastructure of the visa process. To in this case
can comply with article 32 GDPR jo. 32, paragraph 2, under a, VIS Regulation, this is a requirement. BZ has
stated in her opinion that in the spring of 2020 she has passed several systems as critical
to establish. During the opinion hearing on 4 November 2021, BZ presented an (undated) list of
information systems to the AP, after which BZ has indicated which systems are considered critical
infrastructure are identified. NVIS is one of those systems on this list and has therefore been used by BZ
classified as critical infrastructure.
The AP also found during on-site investigations that the Ministry of Foreign Affairs has no emergency plans
drawn up to protect the physical infrastructure of the visa process. The consular post London,
the consular post Dublin and CSO have no further 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 drawing up emergency plans and protecting equipment against disruptions
in utilities, in the opinion of the AP does not comply with the provisions of Article 32, paragraph 1, GDPR and
further elaborated in Article 32(2)(a) VIS Regulation and BIO standards 11.1.4 and 11.2.2.
BZ has stated in its opinion that BZ has concluded that from its own threat analyses
flood detectors and emergency power supplies at the London and Dublin stations are not required.
The AP partly follows this view. Flood detectors can be dispensed with after one
explicit risk assessment. As for power outages, the BIO requires that equipment should be
protected against power outages and other disturbances caused by disturbances in
utilities. Critical infrastructure such as NVIS must be highly secured, with the
interruption of business operations should be avoided as much as possible. BZ has insufficient
explained why NVIS as a critical system does not need an emergency power supply.
The AP also notes that with regard to the rooms at the consulate in London, where work has been done
with visa stickers and the NVIS system, there were physical shortcomings
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 areas in which

work on the visa process in London was not compliant with Article 32(1) GDPR and further elaborated in Article 32(2)(a) VIS Regulation and BIO standards 11.1.1 to 11.1.5 and 11.2.2.

In its opinion, BZ stated (and handed over documentary evidence) showing that in the past measures have been taken for two years to secure access to the consular section.73 [CONFIDENTIAL]. The AP notes that the shortcomings in the field of physical security in the consulate London have now been resolved.

73 Written View of the Ministry of Foreign Affairs 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 largely independent of place and time allowed to work. As soon as work is carried out outside the buildings of Processor 2, the physical security guarantees at the locations of Processor 2 are of course no solution. The legal requirement that personal data of visa applicants may only be processed in areas with adequate physical security, however, remains unaffected. It is unclear to the AP how data within databases of NVIS are physically protected in case of place and time independent work by employees of Processor 2 stationed in both the Netherlands and [CONFIDENTIAL]. The AP has during the investigation received no documentation from BZ that pertains to the physical protection of NVIS data place and time independent work. As the party responsible for processing, BZ must take care of

appropriate security measures for the physical protection of NVIS data, and the
monitor the effectiveness of these security measures.
In its view, BZ states that sufficient security safeguards apply to employees of
Processor 2 working from home. First of all, unauthorized persons do not know where Processor 2 employees live
and the connection to the network and the management VPN is immediately disconnected if a laptop from a
home 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 this context.74
The AP has assessed these regulations and states that work is independent of place and time
state that the employee must take all necessary precautions when using it
personal device in a public place so that the screen cannot be viewed by others.
However, it is not clear what precautions an employee is expected to take. In reaction
the DPA then asked BZ whether and under what conditions employees of Processor 2
are allowed to work with NVIS in public places, how BZ assesses the home working policy of Processor 2 and
which written agreements between BZ and Processor 2 about the physical security of NVIS at places and
time-independent working apply. Finally, the AP has requested a number of audit statements.
BZ has stated that all employees of Processor 2 involved in the NVIS service have the
apply office policies for remote work, which in theory can also take place outside of one's own home
find.75 BZ has assessed Processor 2's homeworking policy as satisfactory on the basis of the already
previously provided employee policies. However, the AP notes that in the BZ submitted
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 assessed working independently of place and time as sufficient.
74 Written View of the Ministry of Foreign Affairs of 15 October 2021, appendices 19 and 20.
75 E-mail BZ dated 10 December 2021.
76 E-mail BZ dated 10 December 2021, appendices 11.1 to 13.3.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

87.

88.

89.

90.

91.

Based on the above, the AP is of the opinion that BZ has not demonstrated that there are 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 - also - of special personal data in NVIS. This makes the nature of the processing is sensitive and the negative consequences for those involved in the event of unlawful processing can be significant. In addition, BZ has the NVIS system as its critical infrastructure marked. While there is a card access system and camera surveillance at the consular posts and CSO applied, such safeguards are not present in public areas.

Now that BZ has not demonstrated that there are sufficient safeguards for physical security at the working in NVIS in public spaces and BZ does not have the effectiveness of the policy on this either checked, the DPA concludes that there is a violation of Article 32 (1) GDPR and further elaborated in Article 32, paragraph 2, sub a and k, VIS Regulation.

2.5 Access rights to NVIS and personnel profiles

2.5.1 Legal framework

Article 6(1) VIS Regulation stipulates that only duly authorized staff of the visa authorities have access to the VIS for entering, changing or deleting visa details. Article 32(2)(f) VIS Regulation requires the necessary measures to be taken established to ensure that only those authorized to consult the VIS have access

to the data to which their access authorization relates and exclusively with

personal and unique user identities (data access control).

Article 32(2)(g) VIS Regulation requires the necessary measures to be adopted to

ensure that all authorities with a right of access to the VIS draw up profiles detailing the tasks and

responsibilities are described of the persons authorized to view data, op

to take, update, delete and search, and make these profiles available upon request and without delay

available to the national supervisory authorities, as referred to in Article 41

(personnel profiles). This is also described in Article 28(4)(c) VIS Regulation which states

that “each Member State is responsible for the management and arrangements under which it is appropriate

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

members of staff and their profile”.

Article 32(2)(k) VIS Regulation requires the necessary measures to be adopted to

verify the effectiveness of the security measures referred to in this paragraph and with regard to

internal control take the necessary organizational measures to ensure that this

regulation is complied with (internal control). This is in line with the generally defined in

Article 32 of the GDPR.

The BIO obliges to allocate management and implementation measures internally. From the

information security policy must show which roles within an organization are responsible for

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

responsible are determined. Specifically, the following provisions of the BIO are 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 access rights to be assigned.

Grant users access

A formal user access grant procedure should be implemented

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

point or retract.

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 upon termination of their employment,

contract or agreement to be deleted, and any changes should make them

amended.

2.5.2 Factual findings

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

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

personnel profiles, authorization procedures and other relevant documentation requested in relation

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 checking access rights

to NVIS?

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

responsibilities of the persons authorized to enter data in the

to view, record, update, delete and search the system? Become NVIS

personnel profiles regularly updated?

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

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

92.

93.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

2.5.2.1 Procedures for granting and checking access rights to NVIS

Consular Post London

BZ has provided three documents to the AP that relate to related authorization procedures

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

NVIS Embassy London'78 and (3)'Work instruction/procedure: logging authorization 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 adopted this manual. In chapter 3 of the document

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

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

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

roles in the department by the Directorate of Consular Affairs and Visa Policy, cluster

Information Management and Control (hereinafter: DCM/MB-IB) is carried out. 80 The document shows

not who is responsible for assigning, changing and checking

authorizations.

The second document consists of one page, is undated and is 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 London consular post gain access to NVIS.81 It also states

document: “In addition to the annual check by business information management, ad-hoc checks (of the

authorizations) at the post.”.

The third document consists of two pages and concerns the control of authorisations. It's in there

stated as follows: “For the purpose of checking logging authorizations, DCV/MB-IB asks the posts and

RSOs once a year (after the annual transfer round) to check which

employees which roles in certain applications should have…”. The document contains further

flowcharts that schematically depict a 'check on application logging authorizations'. It

document is aimed generically and non-specifically at the control of access rights to NVIS. The piece is

undated and has not been established (at a management level).

Based on the inspection at the London consular post, the AP concludes that BZ does not have formal information

has established procedures for granting, changing and terminating access rights to

94.

95.

96.

97.

98.

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

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

79 File document 3, appendix 6b: Work instructions for logging and authorization applications.

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

names of employees

from [CONFIDENTIAL]. ICT manages this technical functionality. No employees can be added manually in NVIS.

An employee only has access to NVIS if he 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 gives access to a specific NVIS component. Manage the tasks at the

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

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

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

Consular Post Dublin

Prior to the investigation in Dublin82, the AP wrote to the BZ83 requesting authorization procedures NVIS and other relevant documentation related to the establishment of access rights to NVIS. BZ has a document entitled 'Authorization procedure NVIS Embassy 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

manager an application to [CONFIDENTIAL]. Access to NVIS is

linked to [CONFIDENTIAL]. The [CONFIDENTIAL] regulates changes of the NVIS accounts and

roll. Furthermore, the annual check of the granted authorizations by [CONFIDENTIAL]

executed.

102.

101. As a result of its investigation at the Dublin consular post, the AP has established that BZ does not have formal

has procedures for granting, changing and terminating access rights to NVIS and for the

checking the granted authorizations to NVIS.

CSO The Hague

During the AP's investigation, the interviewed CSO employees provided an explanation

about the procedure followed by the CSO in 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

the CSO has a work instruction87 [CONFIDENTIAL]. The (undated) work instruction exists

of 13 unnumbered pages. It is unknown whether the document was adopted at the management level.

It does not appear from the document who is formally responsible for granting authorisations

implementing changes to the accounts, assigning NVIS roles and checking them. The AP

concludes on the basis of its investigation at the CSO that it has not been found that BZ has

103.

82 File Document 27: Report of Official Acts OTP Consular Post Dublin.

83 File document 25: Announcement OTP consulate Dublin and Information request AP dated 19 December 2019.

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

85 File document 11: Report of official acts OTP CSO 18 July 2019 and 12 September 2019.

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

87 File document 14, appendix 23.1: Work instruction assigning NVIS roles to CSO.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

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

Processor 2

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

105. The submitted authorization procedures (1 to 4) describe the working method 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, changing and removing access rights to the systems with which Processor 2 works. In addition the authorization procedures address the types of accounts available to employees. By means of a further explanation by BZ during the opinion phase has made it 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

summarily indicated and it is unclear with what concrete actions (e.g. viewing data,

record, update, delete and search) in the NVIS context they accompany. Furthermore, the relationship

between the position of the employee and the assigned NVIS roles and tasks not specified.

107. The DPA has requested BZ to provide personnel profiles94 relating to the

employees of the CSO. BZ has submitted a template text95 with result areas and

competencies, which may be used for the purpose of describing vacancies at the CSO. The

description included in this document does not refer to the duties and responsibilities in relation to

actions in NVIS.

108. During the investigation, the AP established that BZ has not drawn up any personnel profiles in which the

tasks and responsibilities of the staff at the London Consular Post are described,

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

89 File document 17, appendix 8: [CONFIDENTIAL].

90 File document 18, appendix 3: [CONFIDENTIAL]; File document 63: [CONFIDENTIAL]; and File Document 18, Annex 1:

[CONFIDENTIAL].

91 File document 21, appendix 4: Authorization list NVIS.

92 View of the Ministry of Foreign Affairs 14 October 2021, p. 8 and letter BZ to AP dated 19 November 2021, appendix 1

Interview report, p. 33 and 34.

93 File document 5, appendix 1: NVIS profiles.

94 File document 4: AP information request dated 13 June 2019.

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

consular post Dublin and CSO who are authorized to view, update, delete and

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 London consular post to the AP

110.

submitted.

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

access rights to NVIS. The following (multiple) 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 role [CONFIDENTIAL]. On the authorization list that BZ provides to the AP

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

Employee X had not worked for the Consular Section for some time, but he 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 in to the

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

view and mutate current NVIS data.

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

113.

were authorized with mutually incompatible NVIS roles,97 such as those of

[CONFIDENTIAL]. No justification was included in NVIS in which this was awarded

conflicting roles was explained.

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

granted authorizations are checked once a year by [CONFIDENTIAL]. At the consular

post London is [CONFIDENTIAL] responsible for reporting all changes in the NVIS

access rights.98 The operational manager was not present during the investigation and it is unknown

how often the changes regarding 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 DPA has established that at the time of its inspection at the London consular post, an employee wrongly

had access rights to NVIS. This employee was at the time of the AP investigation

appointed to another position at the embassy, for which the use of NVIS was not necessary. Further

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

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

98 File document 7: Report of official acts consular post London.

99 File document 10: AP information request dated 12 July 2019.

several employees of the London consular post had NVIS roles that were mutually exclusive

be incompatible. During the investigation, the AP did not provide any justification for the incompatible roles

NVIS detected and documentation received showing when the last check of the

authorizations and NVIS roles has taken place.

Consular Post Dublin

BZ has submitted an overview of the authorizations granted at the Dublin consular post to the AP.100

At the time of the investigation, six employees were employed at the consular post

had access rights to NVIS, in the following assigned NVIS roles:

[CONFIDENTIAL].

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

The allocation of these conflicting roles in NVIS is at the time of the investigation by or on behalf of BZ

not further motivated.

During the AP's investigation, the employees 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 authorisations.101

CSO

115.

116.

117. The CSO stated during the investigation that the assigned NVIS roles are focused on the

segregation of duties. The roles of registering and deciding are mutually incompatible according to it

functional design of the NVIS application.102

[CONFIDENTIAL]103

The DPA has not found any motivation in NVIS with regard to [CONFIDENTIAL].

118. The overview 'NVIS division of roles per position'104 provided to the AP shows that at the CSO there are 79

employees have access to NVIS. The list includes the following functions:

[CONFIDENTIAL].

These functions have three or more NVIS roles assigned to them. Regarding the role [CONFIDENTIAL]

the investigation by the AP shows that these rolls have not been used for several years.105

119. The above overview also shows that some NVIS roles, about which some employees

of the CSO are regarded as mutually incompatible.106 This concerns the following

NVIS roles: [CONFIDENTIAL].

100 File document 26, appendix 4.1: Employee - Roles - Dublin.

101 File document 27: Report of Official Acts OTP Consular Post Dublin.

102 File document 11: Report of official acts OTP CSO 18 July 2019 and 12 September 2019.

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

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

105 File document 5, appendices 2 and 3 and file document 11.

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

120.

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

During the investigation on July 18, 2019, the CSO stated that the control over the granting of authorizations take place according to an internal control plan. The granted authorizations are updated twice a year checked by [CONFIDENTIAL] every year. In addition, an audit is carried out once a year [CONFIDENTIAL].

[CONFIDENTIAL]107

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

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

122.

123.

The AP also notes that several employees at the CSO have been awarded mutually incompatible NVIS roles, and that [CONFIDENTIAL]employees are left by default 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 came to the conclusion that BZ had not provided any documentation

which shows (sufficiently) which agreements have been made with Processor 2 about the procedures in this respect

of access rights between the controller and processor.

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

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

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

assessed and concludes that no breach of Article 32(2) can be identified on this point

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

2.5.3 Legal Review

Consular posts London and Dublin and CSO

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

CSO have access to NVIS.

[CONFIDENTIAL]

107 File document 14: Response of the Ministry of Foreign Affairs of 8 August 2019 to the AP information request of 25 July

2019. Written answer to the AP's question: 'Who is

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

108 File document 14, appendix 24.1: Management report visa April 2018, version 30 May 2018.

109 Written View of the Ministry of Foreign Affairs of 15 October 2021, p. 8.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

125.

126.

Procedures for granting and checking access rights to the NVIS environment

When granting access rights, including NVIS roles, BZ uses the method described in

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

The Hague. The AP has established that BZ does not have formal registration and deregistration procedures

regarding the assignment to employees of access rights to NVIS. The AP considers that there is

although use is made of a manual for the system,110 containing all sorts of practical information

steps are explained, but that this is not a formally established user access granting procedure

includes with respect to registration and deregistration of authorizations. The other documents111 that as

authorization procedures provided by BZ are an undated, summary description of the

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

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

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

BZ has indicated in its opinion that the existing work instructions will be formalized no later than 1 January 2022

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

the procedure for requesting, changing and terminating access rights in NVIS is sufficient

described.113

Personnel profiles

127. During the investigation, the AP established that BZ had not drawn up any personnel profiles in which the

128.

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

London and Dublin who are authorized to view, record, update and delete data in NVIS

and search. With regard to the provided 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 opinion, BZ states that the access rights allocated to the functions are determined on the basis

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

requested to show this. BZ provided an authorization matrix dated 7 January 2014.116

On the basis of this, the AP concludes that BZ does have personnel profiles that are sufficient

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

In the opinion of the DPA, BZ acted in accordance with Article 32, paragraph 2, under

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 BZ at the time of

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

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

VIS Regulation.

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

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

NVIS authorization procedure

consular post Dublin.

112 Written View of the Ministry of Foreign Affairs of 15 October 2021, p. 6.

113 E-mail BZ to the DPA dated 9 January 2022, BZ process NVIS authorization.

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

115 Written View of the Ministry of Foreign Affairs of 15 October 2021, p. 7.

116 E-mail BZ dated 10 December 2021, appendix 14.

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

Control of access rights to NVIS

129. The AP has first established that BZ has no formal procedures with regard to the

periodically checking the granted access rights to NVIS and NVIS roles. From the by BZ
provided documentation118 shows that the granted authorizations are checked once a year by [CONFIDENTIAL]
are checked. In addition, it has been stated that internal checks are carried out at the consular
posts in London and Dublin and at the CSO.119

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

131.

132.

133.

evidenced by the checks by [CONFIDENTIAL]. Nor has BZ shown when the most recent
check has been performed. With regard to the internal controls, the AP considers that in the case of the
consular post London no documents have been provided that pertain to the internal controls of the granted
authorizations. With regard to the CSO and the Dublin consular post, the AP concludes on the basis of the
provided information120 that there were some internal controls related to past authorizations
have occurred. The last internal audit at the CSO took place in April 2018. The consular
postal Dublin carries out checks at least once a year; the last check was done in 2019.121
The AP has also 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 turned out to be
had not been used for some time. This points to the fact that the access rights granted to
NVIS and NVIS roles are insufficiently checked.
During the opinion hearing, 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 the Ministry of Foreign Affairs of the checks [CONFIDENTIAL]
of the London and Dublin Consular Post have performed access rights to NVIS from 2018 to
with 2021. In response, BZ provided the following: 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 provide a general picture of the screening of consular posts (from 2018 and 2019). The by BZ

documents submitted do not lead the AP to a different conclusion. The AP establishes that BZ does not have

demonstrated that the operational managers of the consular post London and Dublin regularly checks

performed on the access rights to NVIS.

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

Authorization procedure NVIS Consular post

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

119 File document 7: Report of Official Acts Consular Post London; File document 27: Report of official acts consular post

Dublin;

and File document 11: Report of CSO official acts July 18, 2019 and September 12, 2019.

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

2018; and File document 27, appendix

6: 6. Correspondence about adjusting NVIS roles.

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

122 Letter from BZ to AP dated 19 November 2021, appendix 1 Interview report, p. 30.

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

that it describes the process surrounding the one-off autumn inspection of [CONFIDENTIAL].123 De

AP notes that no clarity is provided in these proceedings about how BZ will ensure this

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

sets, like a safety net. Given the type of data processing in NVIS, the AP considers an annual check

insufficient to ensure that only authorized employees have access to this system. This working method insufficiently mitigates the risk that an employee who changes jobs will be at risk for months improperly accesses NVIS, [CONFIDENTIAL].

135. The AP has also established that an employee at the London consular post was wrong about had access rights to NVIS in the role of [CONFIDENTIAL], and could therefore access NVIS data view and change. This employee had been appointed to another position at the embassy, for which the use of NVIS was not necessary. BZ has stated in its opinion that the [CONFIDENTIAL] application was flawed at the time of the investigation, as a result of which the role [CONFIDENTIAL] is still to be preserved in case the [CONFIDENTIAL] application fails. This argument fails. An employee who has not worked in the consular section for some time, should not have access to NVIS. As for the [CONFIDENTIAL] role, the AP follows the view of BZ that the finding on this subject had an incorrect source reference. The concerned finding related to employees of CSO and has corrected the AP above source credit corrected.

136. Finally, during the investigation, the AP established that a justification for granted irreconcilable roles within NVIS is missing. BZ states in its view that in some cases this does not occur conflicting roles may be assigned to a person. This could be about, for example smaller posts where an employee suddenly drops out. According to BZ, the motivation is conflicting roles are documented. As a result, the AP has requested documentation about the responsibility and motivation for assigning incompatible roles. Based on this the AP notes that BZ has shown several examples that show that BZ has irreconcilable roles in has motivated the past.124 With regard to this point, the AP follows the view of BZ. The AP has however, cannot see a policy that shows how BZ deals with incompatible roles and how BZ defines incompatible roles. The NVIS Data Management Manual only states that the incompatible roles in NVIS are currently not set.125 Policies regarding segregation of duties are 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 about access rights

to the NVIS environment and the control thereof, violates Article 32, paragraph 1 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 on the Plan-Do-Check-Act cycle).126

123 E-mail BZ to the DPA dated 9 January 2022, BZ process NVIS authorization.

124 BZ email dated 10 December 2021, appendices 20 and 20.1 and the written Opinion BZ dated 15 October 2021, appendix

22.

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

126 This means that it is necessary to check regularly whether the security policy is still being observed in practice and

whether the measures are still

to fulfil. Should imperfections come to light, the Plan-Do –Check-Act principle from the BIO – in short – requires that errors

2.6 Monitoring NVIS Usage: Log Files

2.6.1 Legal framework

138. The obligation to keep and regularly check log files is an essential one

139.

part of the information security regulations. In this way, an organization can monitor it

keep track of which employee consults or changes certain information when and for what purpose. It is

it is also necessary that periodic monitoring of the recorded log files takes place in order to

to be able to detect unusual patterns and, for example, to check whether unauthorized

access to the data.

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

which personal data have been processed in NVIS, when, by whom and for what purpose. BZ also needs the

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

take necessary organizational measures. Article 32(2)(f) VIS Regulation prescribes that

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

their access authorization relates, and only 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 regularly review these log files. The BIO standards

specify which information about NVIS usage should be kept in a log file as a minimum

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:

Register events

Event logs that identify user activities, exceptions

and record information security events should be

are created, stored and regularly reviewed.

A log line contains at least:

a. the event;

b. the necessary information required to report 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

repaired and that the policy is adjusted in such a way that the problems in question will not occur again in the future. The the results of the on-site inspection by AP inspectors described above show that this did not happen with regard to authorizations and role management. This means that there is no adequate internal control in the area of access security. This may arise

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

2.6.2 Factual findings

141. In order to check compliance with the 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, of CSO and of Processor 2. During the on-site investigations, the AP also127 questions were asked about the design 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 ones authorization lists that relate to the same period.

Logging of NVIS usage at consular posts London and Dublin

[CONFIDENTIAL]

[CONFIDENTIAL]128

Log file analyses

142.

143.

144. The DPA requested two log files regarding the use of NVIS by the employees of the London Consular Post. The first file (hereinafter referred to as: Log 1) concerns the log file of 4 July 2019, between 9 a.m. and 12 p.m. This period coincides with the AP's investigation on site. It

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

[CONFIDENTIAL]129

[CONFIDENTIAL] 130

145.

146.

127 On-site investigations at the London consular post (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 View of the Ministry of Foreign Affairs of 15 October 2021, Appendix 2 under number 6.3.

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

130 File document 16, appendix 8.1: LON_01April2019_04July2019_Overview.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

Logging of NVIS use 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, where the subject NVIS logging has been investigated. The AP also has additional documentation on this subject at BZ retrieved132 and analysed. In addition, the AP has carried out analyzes of log files.

Process of logging and checking log files

[CONFIDENTIAL]133

[CONFIDENTIAL] 134 135

147.

148.

149.

131 File document 11: Report of official acts OTP CSO 18 July 2019 and 12 September 2019.

132 File document 13: AP request for information dated 25 July 2019; and File document 17: AP information request dated October 1, 2019.

133 File document 11: Report of official acts OTP CSO 18 July 2019 and 12 September 2019.

134 File document 13: AP information request dated 25 July 2019.

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

150. The AP has requested (extensive) security documentation 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 analyses

151.

152. The DPA also requested NVIS log files 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 which relate to the following periods:

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

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

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

[CONFIDENTIAL]

[CONFIDENTIAL]145

136 File document 14, appendix 14.1: [CONFIDENTIAL]

137 File document 12, appendix 44b: [CONFIDENTIAL]

138 File document 14, appendix 16.1: [CONFIDENTIAL]

139 File document 14, appendix 16.2: [CONFIDENTIAL]

140 File document 14, appendix 19.1: [CONFIDENTIAL]

141 File document 14, appendix 19.2: [CONFIDENTIAL]

142 File document 16, Appendix 9.1: CSO_01Sept2018_30Nov2018_Overview.

143 File document 16, appendix 9.2: CSO_01April2019_18Juli2019_Overview.

144 File document 16, appendix 9.3: CSO_12Sept2019_Overview.

145 Written View of the Ministry of Foreign Affairs 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 has analyzed some log files of Processor 2. The AP establishes that, through the lack of sufficient evidence about the actual situation in combination with the explanation of BZ, for what regarding the contents of these log files, no violation can be detected and will therefore not continue be dealt with in the legal review below.148

2.6.3 Legal Review

159. The AP has assessed the extent to which 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 number of other data are recorded related to actions in NVIS, such as an indication for some steps under it visa process (e.g. [CONFIDENTIAL]).

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

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

148 Written View of the Ministry of Foreign Affairs of 15 October 2021, p. 11.

161. Log 1 does not show which actions in NVIS are by the employees of the London consular post 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 employees of the consular post, with what purpose, when this took place and what device was used for this. The AP states

also found that there are discrepancies between the two log files. Since Log 1 is about July 4, 2019 and Log 2 covering the period July 1, 2019 through July 3, 2019, Log 2 and Log 1 are chronologically connected. However, both files differ in structure.149

In Log 3, Log 4 and Log 5, in addition to the name of the employee, the visa application number and a global indication of the part of the visa process that was carried out and the time at which it was carried out 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 occurred.

162.

163. In view of the above findings, the AP notes 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 the structure and type of data contained in them inconsistencies.150 Moreover, the log files that the AP received and assessed show that not all mandatory actions are logged. [CONFIDENTIAL]151

In its opinion (insofar 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 the way of the AP to inform BZ on it point out that not only the log data about the access was requested, but also which actions in NVIS have been performed and at what time. This argument fails. The AP has a log file in its information request asked about the use of NVIS at the London embassy.152 In the AP's opinion, it is necessary little argument that when using NVIS, in which - undisputed - personal data are processed, the AP is not just interested in information about logging into this system.

164.

165. With regard to log file 2, BZ argues that Article 32(2)(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 which data is being processed can therefore, according to BZ, suffice without an exact representation of that data. Meaning comes into play

Article 32 GDPR. The purpose of the logging is to check the lawful use of access rights. Because

BZ records which application data is processed, so it is sufficiently clear which

data has been processed. According to BZ, the visa application number also indicates which person is involved

personal data has been processed. It would be going too far to determine for each visa applicant whether the

For example, NVIS employee has only processed 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 OTPs CSO on 16 July 2019 and 12 September 2019 (see file document 11: Report of

Official Acts OTP

CSO 16 July 2019 and 12 September 2019).

152 File document 10, appendix 1 under point 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 check and determine which data, when, by whom and for what purpose

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

data are processed. As a result, it is not possible to see afterwards 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

are. In this context, in which a great deal of - also - 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 have been changed, not only after an incident. This information may also be from a combination of

(log) files can be derived. The purpose of logging is therefore not limited, as BZ states, to the

control of lawful use of access rights.

BZ also states in its written opinion that the AP's conclusion 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 believes that it
request for information about this by the AP was formulated too generally. According to BZ there are many in NVIS
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 this was controlled in the security policy
tuned in.

167.

168. Although the AP is of the opinion that it is for the Ministry of Foreign Affairs to timely - and not just in an opinion -
the AP BZ has another opportunity to indicate that a request for information raises questions
required to submit procedures that describe how BZ logs with respect to NVIS and
carries out checks on this.153 BZ has issued an undated document with a few paragraphs in response to this
provided with a factual description of what is logged when using NVIS.154
[CONFIDENTIAL]155

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

2.7 Monitoring NVIS Usage: Security Incidents

2.7.1 Legal framework

Article 32(2)(c) and (d) of the VIS Regulation stipulates that BZ is appropriate
takes measures to prevent data carriers from being unlawfully read, copied,

170.

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

154 Email BZ to AP dated 10 December 2021, Appendix 16.

155 See section 2.6.2 and letter BZ to AP dated 19 November 2021, appendix 1 Interview report, p. 36.

changed or deleted, and that data is unlawfully accessed, changed or deleted. If 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) of the VIS Regulation states that the necessary organizational measures have been taken should be for the follow-up of such security incidents. So write these provisions for internal checks on the NVIS data carriers and the storage of NVIS data to 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 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:

prompt, effective and orderly response to information security incidents

to accomplish.

Information security event reporting:

Information security events belong through the right as soon as possible

management levels to be reported.

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

There is a reporting procedure that specifies the duties and responsibilities of the reporting desk

described.

All employees and contractors have demonstrably taken note

of the incident reporting procedure.

The process owner is responsible for resolving security incidents.

Incident follow-up is reported monthly to the person responsible.

Information security vulnerabilities reporting:

From employees and contractors who use the information systems and

services of the organization should be required to provide systems or services

record and

report.

Lessons learned from information security incidents:

Knowledge obtained by analyzing information security incidents

and solve ought to be used to determine the probability or

reduce the impact of future incidents.

Security incidents are analyzed with the aim of learning and

prevent future security incidents.

171.

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

be accomplished of information security incident management, including

communication about security events and security vulnerabilities. To serve this purpose

responsibilities and procedures must be established, a reporting desk must 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 person responsible on a monthly basis. Be for this

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

172.

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

prevent security incidents.

2.7.2 Factual findings

As part of its investigation, the AP has checked whether BZ has a procedure for the

reporting and following up on security incidents/data leaks 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 on security incidents

requested.

Consular posts: London and Dublin and CSO The Hague

Security incident procedure

173. The London and Dublin consular posts and the CSO follow the same Ministry-wide working method with regard to this

174.

to reporting security incidents/data leaks: a security incident will be 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 employees [CONFIDENTIAL].

On site at the consular posts, employees also use 'Fact sheets data leaks' 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 the steps that employees must follow in the event of a data breach.

During the investigations, the aforementioned data breach factsheets 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, in both Dutch and English. See these factsheets

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

displayed at the consular posts.

Instructional videos about data leaks158: these short films provide information about

data leaks.

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

of data leaks159 and the description of the procedure for BZ employees in the event of

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

156 File document 10: AP information request dated 12 July 2019.

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

File document 12, appendix 11d: Sharepoint data leaks.

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

video files.

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

160 File document 12, appendix 12c: Data breaches of information for BZ employees.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

BZ must take in the event of data breaches, in accordance with the procedure established during the studies in London and Dublin has been explained.

176. The AP notes that the employees of the London and Dublin consular posts and the CSO, with regarding reporting security incidents/data breaches, follow the procedure set out for all employees of BZ applies. This procedure is a hands-on guide on the steps involved employees must take action in the event of security incidents: these must be dealt with as quickly as possible [CONFIDENTIAL] are reported and in case of data breaches a report is made to [CONFIDENTIAL]. The mentioned procedure has not been established at a management level, and gives no further 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 reports

of incidents162 at the London consular post. [CONFIDENTIAL]. By the lack of

a further explanation of these reports, the AP assumed during the investigation that BZ

has not provided a copy of the security incident register.

[CONFIDENTIAL]163

[CONFIDENTIAL] 164

180.

161 File document 10: AP information request dated 12 July 2019.

162 [CONFIDENTIAL]

163 [CONFIDENTIAL]

164 File document 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 has a

incident register in which security incidents are recorded. The AP has asked

to provide a security incident register related to NVIS and regarding 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 requested a semi-annual report on security incidents. This

document has been provided.166 It describes data leaks related to travel documents.

During the opinion phase, BZ provided the following explanation about the process of, among other things

security incidents. Reports are handled by [CONFIDENTIAL] in [CONFIDENTIAL].

All actions required to handle a report are recorded herein and

stored. These reported incidents/infringements, regardless of whether they had reported them to the AP must be completed, are closed, logged and stored in a shielded environment accessible only to [CONFIDENTIAL] behind the [CONFIDENTIAL] (the data leak register). All (subsequent) steps performed are recorded in the individual notification 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 location are tracked and stored.

183. In response to the above, BZ has answered further questions from the AP about the design of the central register of security incidents. On this basis 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. receive 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 there were and 2019 there have been no incidents in relation to the NVIS environment. This specifically related to incidents [CONFIDENTIAL]

165 File document 14, appendix 20.1: Explanation.

166 File document 14, appendix 21.1: [CONFIDENTIAL].

167 File document 17, appendix 3: Incident Escalation Procedure.

168 File document 17, appendix 4: [CONFIDENTIAL].

169 File document 17, appendix 5: Procedure Data Breach Controller.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

186. When asked whether Processor 2 keeps a log or register of security incidents, Processor 2 has declared 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 have been with respect to NVIS during the study period. As a result, there were no internal reports which Processor 2 could provide to AP.172

187.

188. Based on the above and the explanation provided by BZ during the opinion stage, the DPA considers the division of tasks between BZ and Processor 2 with regard to security incidents is sufficiently clear.

2.7.3 Legal Review

189. The AP comes to the conclusion 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 one no more than a manual on the steps that employees should take in case of security incidents: these must be reported to [CONFIDENTIAL] as soon as possible and in case data leaks are reported to [CONFIDENTIAL]. The mentioned procedure is not finished 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 neither are the duties and responsibilities of the reporting desk and who is responsible as process owner is for resolving security incidents and reporting on them.

During the opinion phase, BZ responded to this with a GDPR manual (approved on 13 October

2021) and a Process description Incident management security incidents and data leaks (July 2020)

provided to the AP. The AP has assessed this documentation and has come to the conclusion that BZ from 13

October 2021 does provide full insight into the steps that are followed after a report about

a security incident/data breach has occurred. The duties and responsibilities of

the reporting desk and BZ has determined who, as process owner, is responsible for the

resolving security incidents and reporting on them.

190.

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

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

172 Written View of the Ministry of Foreign Affairs of 15 October 2021, p. 13.

191. Based on 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 breached the requirements laid down in Article 32(1) GDPR and

further elaborated in Article 32(2)(c) and (d) of the VIS Regulation and 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 is therefore on this

point ended.

2.8 Staff training on personal data protection

192. Article 28(5) VIS Regulation requires that authorities' staff with a right of access to

the VIS should receive proper training on data security and data protection rules.

Staff are also informed of relevant criminal offenses and sanctions. The AP

however, has not tested the content of these courses or the way in which they are offered
during the investigation. Article 38(3) Visa Code further stipulates that the “Central Authorities of
Member States [should] appropriately train and
provide them with complete, accurate and up-to-date information on relevant legislation.”

193. The AP concludes 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 data protection and security training. In addition, the training courses
offered for both employees who have only recently joined BZ and employees who have been with BZ for a longer period of
time
to work. The training includes, among other things, the systems to be used (including NVIS), relevant laws and regulations
regulation and security. The AP also notes that there are training programs of both seconded and
local employees.

194. This concludes, with regard to the question of whether attention is paid to
information security and the regulations on the processing of personal data, the requirements have been met
laid down in BIO target 7.2.2 and Article 38(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 fair
data processing. Informing the data subject about data processing contributes to this
transparency. Article 37 VIS Regulation requires visa applicants to be informed of the
responsible, 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
collection of this data and the rights of the data subject. This means that BZ the visa applicants

195.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

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

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

2.9.2 Factual findings

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

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

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

Information is provided by means of (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 of 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 BZ.178 website

The Privacy Statement deals with various privacy components 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

data subjects. A separate document lists the high-risk countries that could affect the

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

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

area and agencies 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

visa application process. The AP further notes that the national "Data Protection Authority",

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

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

199. The second option of providing information takes place via the Annex.181 The Annex becomes

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

collected. In the Annex, BZ is named as the controller for the processing

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

retention periods and becomes the obligation to collect the personal data

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

the

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

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

175 File document 7, appendix 6: Schengen Visa Application (example form), issued attn. the OTP consular post London.

176 File document 7, Annex 4: Information sheet on SIS II; and File document 27, appendix 10: Leaflet public information

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-visa (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 14 august 2020).

178

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

-en (for

last accessed 23 February 2022).

179 In accordance with Article 22 Visa Code.

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

181 File document 7, appendix 6: Schengen Visa Application (sample form), issued attn. the OTP consular post London.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

explained. Reference is also made to the Dutch Data Protection Authority for complaint 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 during the investigation in Dublin,182 when the

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

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

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

during the visa application process. Although 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 those involved in the visa process.

2.9.3 Legal Review

201. The DPA notes that BZ describes the purposes of the data processing in the Privacy Statement and in the Appendix (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, this applies 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 Annex make no mention of sharing personal data with third parties

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

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

13(1)(e) GDPR.

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

203. The AP does not follow BZ's position. It follows from Article 13(1)(e) GDPR that the controller informs the data subject about the recipients or categories of recipients of the personal data. Article 4, part 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 Document 27: Report of Official Acts OTP Consular Post Dublin.

183 File document 7, Annex 4: Information sheet on SIS II; and File document 27, appendix 10: Leaflet public information about SIS II..

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

185 Article 29 Data Protection Working Party Guidance on Transparency under Regulation (EU) 2016/679, p. 18.

2.10 Conclusions

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

Security plan

205. The AP comes to the conclusion that BZ has no security plan with regard to NVIS (and therefore

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

Articles 24 and 32 (1) GDPR, which are further elaborated in Article 32 (2), opening words, VIS Regulation and BIO-

standards 5.1.1, 5.1.1.1 and 5.1.2.1.

Physical security

206. BZ has, by not explicitly determining which parts of the IT infrastructure should be classified

as the critical infrastructure of the visa process, from at least September 1, 2018 to every

case spring 2020 violated Article 32 (1) GDPR, which is further elaborated in Article

32(2)(a) VIS Regulation.

207. The AP also concludes that BZ, when it comes to drawing up emergency plans and the

protection of equipment against disturbances in utilities, from at least September 1, 2018

to date does not comply with the provisions of Article 32 (1) GDPR, which is further elaborated in Article 32 (2)

sub a, VIS Regulation and BIO 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 being done on the

visa process in London was not satisfactory. As a result, BZ has from at least 1 September 2018 to April 2020

contravened Article 32(1) 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 BZ has not demonstrated that there are sufficient safeguards for physical security

working in NVIS in public spaces and BZ does not have the effectiveness of the policy on this either

checked, the AP comes to the conclusion that BZ has been in violation from at least September 1, 2018 to the present

acts in accordance with Article 32, paragraph 1, GDPR, which is further elaborated in Article 32, paragraph 2, sub a and k, VIS

Regulation.

Access rights to NVIS

210. The AP comes to the conclusion that from at least September 1, 2018 to January 1, 2022, the Ministry of Foreign Affairs

has no formal

registration and logout procedures in place regarding the assignment of access rights to

NVIS. With this, BZ has acted contrary to article 32, paragraph 1, GDPR, which is further elaborated in BIO-standards 9.2.1 and 9.2.2.

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

Control NVIS usage: logging

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

Control NVIS Usage: Security Incidents

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

Information provision to visa applicants

214. Finally, the AP comes to the conclusion that BZ is involved in the provision of information visa applicants do not report the sharing of personal data with third private parties,

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

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

3 Fine

215.

216.

217.

3.1 Introduction

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

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

as referred to in Article 5 GDPR. The AP uses her for the established violations

authority to impose a fine on BZ. BZ stated in its opinion that by various

transition processes and improvement measures, the imposition of a fine and/or an order subject to periodic penalty payments

is not

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

the AP, unlike BZ, considers the fact that the violations are still continuing to impose a fine and a

burden under penalty is appropriate. The AP motivates this in the following.

3.2. Penalty Policy Rules of the Dutch Data Protection Authority 2019

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

connection with Article 14, third paragraph, of the UAVG, the AP is authorized to inform BZ 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, opening words and under i and Article 83, fifth paragraph, of the GDPR, read in

connection with Article 14, third paragraph, of the UAVG, the AP is authorized to inform BZ 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 Fining Policy Rules regarding the implementation of the aforementioned power to imposing an administrative fine, including determining the amount thereof.186 In the Penalty 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 fine bandwidth between € 120,000 and €500,000 and a basic fine of €310,000. Violation of Article 13 of the GDPR has been classified in category III. Category III has a fine range between €300,000 and €750,000 and a basic fine of €525,000

219. The AP adjusts the amount of the fine to the factors referred to in Article 7 of the Penalty policies, by lowering or increasing the base amount. It is an assessment of the seriousness of the offense in the specific case, the extent to which the offense can be imposed on the offender and, if there is reason to do so, other circumstances.

3.3 Fine amount for violation of the security of the processing

220. Any processing of personal data must be done properly and lawfully. To avoid that organizations with the processing of personal data infringe on the privacy of citizens

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

It is very important that they apply a security level appropriate to the risk. 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 to 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 the personal
mean privacy, stricter requirements are imposed on the security of personal data. The
AP has concluded that BZ does not have a sufficiently risk-oriented security level
guaranteed and guaranteed in the context of processing Schengen visa applications.

3.3.1 Nature, seriousness and duration of the breach

221. The AP has established that BZ processes a great deal of (sensitive) personal data of data subjects.
Examples of this are the combination of name and address details, country of birth, purpose of the trip,
nationality and photo. Those involved are obliged to provide all this personal data to BZ in order to
to obtain a Schengen visa. In such a dependent and unequal position it is of
It is of great importance that BZ sufficiently guarantees and safeguards a security level geared to the risk. The
This is because the consequences and the resulting damage for those involved are great in the event of loss,
alteration or unlawful processing of the data. For example, unauthorized persons can
view and change personal data, but also authorized employees can during the treatment
of the application make input errors. As a result, applications can be wrongly refused, which again
constitutes an infringement on the freedom of movement of those involved. 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 consideration that BZ processes personal data of very many data subjects.
It has been 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 requests are therefore insufficiently secured. Finally
the AP notes that the violation has been going on for 3.5 years and is still continuing. The AP considers this
extremely serious.

223. In view of the above, the AP sees, pursuant to Article 7, preamble and under a, of the Fining 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 Breach

224. BZ is obliged to maintain a security level that is appropriate for the nature and size of the processing carried out by BZ. Now that BZ has not guaranteed an appropriate level of security for many years, the AP is of finds that BZ has been and continues to be seriously negligent in taking appropriate action security measures and checking and adjusting these measures. Citizens who oblige to provide personal data, must be able to assume that BZ, as a government agency, has the has taken and is taking 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 already identified risks in its own analyzes (from 2015 and 2020). area of information security with regard to NVIS and has not been detected in a timely manner and/or has taken insufficient action.188 For example, in 2015, if in 2020 the Ministry of Foreign Affairs defined that as a result of power failures equipment can malfunction and that unauthorized persons being able to perform changes in NVIS as a result of insufficient governance with regard to authorizations. The AP also refers to the accountability audits by the Court of Audit on this point 2017, 2018 and 2019, from which it follows that the deficiencies in information security for BZ also were already known for this reason. The Court of Audit has established that BZ runs risks on the focus areas governance, the structure of the organization and risk management. Also has the The Netherlands Court of Audit has ruled that the Ministry of Foreign Affairs has no management framework for the implementation and implementation of

properly initiate and manage information security within the organization.

226. In view of the above, the DPA sees, pursuant to Article 7, preamble and under b, of the Fining 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 BZ in the context of processing applications for Schengen visas processes special personal data, such as fingerprints. Such data qualifies as biometric data. Special personal data requires even higher protection. The AP BZ has determined that BZ is insufficiently at risk for a very large group of people involved applies an appropriate security level for this category of special personal data.

228. In view of the above, the AP sees, pursuant to Article 7, preamble and under g, of the Fining Policy Rules reason to increase the fine to € 465,000.

3.4 Fine amount for violation of information provision to data subjects

229. The controller should provide the data subject with information necessary to to guarantee fair and transparent processing vis-à-vis the data subject, with due observance of the specific circumstances and the context in which the personal data are processed.189 The AP has established that BZ does not make any notifications in the context of the provision of information to visa applicants makes of the sharing of personal data with third private parties and thus Article 13(1)(e) GDPR violation.

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 been going on for 3.5 years and is still continuing, the AP considers that an administrative fine should be imposed appropriate.

188 File document 3, appendix 5a: Vulnerability analysis and DCV IS plan; Written View of the Ministry of Foreign Affairs of 15 October 2021, Appendix 3.

189 See recital 60 of the GDPR.

231. With regard to the amount of the fine, the AP takes into consideration that the consequences of this violation

232.

be limited. This means that the AP sees reason to adjust the basic amount from the point of view of proportionality

to reduce the fine from € 525,000 to € 100,000.

3.5 Culpability and Proportionality for Both Offenses

Pursuant to Section 5:46(2) of the Awb, when imposing an administrative fine, the AP

take into account the extent to which this can be attributed to the offender. Now that this is one

violation, it is not required for the imposition of an administrative fine in accordance with established case law

it is demonstrated that there is intent and the AP may assume culpability if the

perpetrator is established.

233. BZ is obliged to use appropriate technical and organizational measures to prevent a risk

appropriate level of security. In addition, BZ must be sufficiently clear to those involved

determine to which parties it provides personal data. BZ can be blamed for not addressing this one

meets two obligations. The GDPR, 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

that organizations must maintain a level of security appropriate to risk. Furthermore, the GDPR (en

do the guidelines on transparency) provide sufficient explanation as to what information is

stakeholders should be shared. BZ may be expected to follow the rules applicable to it

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 given the circumstances of the specific case, not to one 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 took 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 those involved 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 provision of information to data subjects, the AP has already explained in paragraph 3.4 why the imposed fine is, in its opinion, proportionate.

236. In view of the foregoing, the AP sees no reason to increase the amount of both fines on the basis of the proportionality and the circumstances referred to in the Fining Policy Rules, insofar as applicable in the case, further increase or decrease.

3.6 Conclusion

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

190 See also sections 3.3 and 3.4 for the justification.

4. Order subject to periodic penalty payments

238. As it concerns 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 lays down on the basis of Article 58 (2) opening words and under d GDPR jo. Article 16, paragraph 1, UAVG and Article 5:32, paragraph 1, Awb to the Minister also issued an order subject to periodic penalty payments.

239. The AP orders the Minister of Foreign Affairs to handle applications from

Schengen visas:

1. end the violation of Article 32 (1) GDPR by appropriate technical and organizational measures

take measures to ensure a level of security appropriate to the risk.

To this end, the Minister serves for the national information system for the purpose of processing

from Schengen visa:

draw up an information security policy that also states how BZ implements this policy

periodically reviewed and adjusted if necessary.

b. prepare contingency plans and protect equipment against disruptions

utilities.

c. take sufficient guarantees for physical security when working in this national

system in public areas.

d. to record how BZ guarantees regular checks on access rights to this system.

This also means that access rights must be regularly checked and

be adjusted immediately if an audit shows that an employee is wrong

authorized to access personal data.

e. to ensure that it is possible to check and determine which data, when, by

who and for what purpose have been processed.

f. to record the manner in which BZ logging and regular checks are carried out in this system

guarantees. This also means that BZ must regularly check log files.

It is up to the Minister, as controller, to determine the exact details of this

the aforementioned remedial measures.

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

The Minister must 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 period and amount of penalty with regard to part 1

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

241.

If the Minister for Foreign Affairs does not meet the burden before the end of this grace 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 term set by the Minister

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

€500,000.

Favorable period and amount of penalty with regard to part 2

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

243.

efforts are involved. The AP therefore attaches an end-of-benefit period to Part 2

March 24, 2022.

If the Minister for Foreign Affairs does not meet the burden before the end of this grace period

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

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

Secretary of State 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 applies to 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

data subjects. Furthermore, the AP considers the amounts to be high enough to persuade BZ to commit the violation

to end.

245. The above measures are within the power of BZ to take and the term for taking these measures
the AP considers realistic. The AP has taken into account that a large part of the
measures to be taken by BZ in Part 1 primarily comprise the preparation of documentation. And for
with regard to component 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 grace period has expired
prevent, the AP suggests BZ to consider the documents – with which BZ can demonstrate that it complies
to the burden – in good time, but no later than one week before the end of the beneficiary period to the AP ter
send review.

246.

247. Finally, the DPA suggests that the Ministry of Foreign Affairs regularly communicate on the basis of a concrete schedule
inform the AP about the progress of the measures it is taking to comply with Part 1
of the imposed load.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

5. Operative part

The AP has come to the conclusion that the Minister of Foreign Affairs, as
controller in the process of issuing Schengen visas, data subjects
insufficient information and the security of the processing of personal data is insufficient
guarantees. Given the fact that the Minister of Foreign Affairs has a lot 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 breaches of the GDPR as serious.

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

a burden under duress.

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

and Article 13, paragraph 1 under e, GDPR, an administrative fine in the amount of: € 565,000 (in words:

five hundred and sixty-five thousand euros).191

- The AP orders the Minister of Foreign Affairs to handle applications

from Schengen visa:

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

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

to end; and

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

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

violation of Article 13(1)(e) GDPR.

If the Minister of Foreign Affairs does not comply with the

obligation, 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, to a

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

If the Minister for Foreign Affairs does not comply with the

obligation, 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 last day of the stipulated

term, within which the Minister of Foreign Affairs fails to comply with part 2 of the order, 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 should be

accordingly

Article 4:87, first paragraph, Awb must be paid within six weeks. For information and/or instructions about payment, please

contact

be recorded with the previously mentioned contact person at the AP.

59/64

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

Yours faithfully,

Authority for Personal Data,

e.g.

ir. M.J. Verdier

Vice President

Remedies Clause

If you do not agree with this decision, you can within six weeks from the date of sending it

decides to submit a notice of objection digitally or on paper to the Dutch Data Protection Authority. In accordance

Article 38 of the UAVG suspends the effect of the decision until submitting a notice of objection

imposition of an administrative fine. Submitting a notice of objection suspends the effect of the order

subject to penalty 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 submission on paper

is: Dutch Data Protection Authority, PO Box 93374, 2509 AJ The Hague. Mention 'Awb objection' on the envelope

and put 'objection' in the title of your letter. Write in your notice of objection at least:

- your name and address;

- the date of your objection;

- the reference referred to in this letter (case number); or enclose a copy of this decision;

- the reason(s) why you disagree with this decision;

- your signature.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

ATTACHMENT 1

The following legislation forms the basis of the legal framework for this decision:

 The General Data Protection Regulation (GDPR) determines 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 with data on short-stay visas (hereinafter: VIS Regulation192).

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 authorities are responsible for data processing via the VIS. The

VIS Regulation prescribes which data of data subjects who have a visa for it

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

the parties responsible for using the VIS.194 This includes, among other things

guarantees in the field of integrity and confidentiality of the visa information.195

 The Regulation establishing a common visa code (hereinafter: Visa Code)196

outlines the general framework that Member States must comply with in the context of the applications

issuance of visas.197 This framework determines, among other things, which data must be processed for the

applying for and issuing a visa for the Schengen area and various preconditions

which the Member States must comply with in this process.

The AP has assessed this 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 discussed is the concept of “personal data”, the processing of personal data, the controller and the processor.198

192 Reference: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008R0767

193 See Article 9 of the VIS Regulation

194 See, for example, Articles 1 and 47 of the VIS Regulation

195 See, for example, Articles 1 and 28 of the VIS Regulation

196 Reference: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32009R0810

197 Article 1 Visa Code: This Regulation lays down the procedures and conditions for issuing visas for transit across the territory of the Member States or an intended stay in the territory of the Member States not exceeding three months in any 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 met in order to process personal data in accordance with the Regulation. Especially 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 decision, in the specific legal framework relating to visa information systems.

Security of processing

Article 32 GDPR prescribes - in short - for that controller and the processor must take appropriate technical and organizational measures to ensure a risk-based approach to ensure a level of security. The general standard regarding securing personal data in Article 32 GDPR means that the controller, taking into account with the state of the art, the implementation costs, as well as with the nature, size, context and the processing purposes and the varying likelihood and severity of risks to the rights and freedoms of persons, must take appropriate technical and organizational measures to protect it risk-appropriate level of security.

The term 'appropriate' also indicates a proportionality between security measures and the nature of the data to be protected. As data has a more sensitive character, or the context in which it be used mean a greater threat to privacy, be heavier requirements for the security of this data.199

In order to further determine which security measures are appropriate, they apply in most sectors more specific information security standards. Most relevant security standards for the government are contained in The Baseline Information Security Government (BIO).200 The BIO is complete 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 has these standards unless there are explicit reasons not to do so.

The AP notes that the Baseline for government information security has been in effect since January 1, 2020. Herein 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 were

further elaborated in the Baseline Information Security of the Government Service (hereinafter: BIR). The BIR is as well

based on the ISO 27002 standards and valid until the end of 2019.

The AP has the state of the security of data processing through the national

Visa Information System also specifically assessed against Article 32(2) VIS Regulation. This article looks at it

taking security measures, including a security plan. These provisions from the VIS

199 Dutch Data Protection Authority: Policy rules for the security of personal data, February 201 3, p. 1 0 and Parliamentary

Papers II 1 997-1 998, 25 892,

no. 3, p. 99.

200 The Government Information Security Baseline (BIO) is the leading standard for the government. In this case, its

predecessor is also the

BIR is important because the BIR was the standard from the start of the study up to and including the end of 2019. Both

standards are based on the

ISO27000 information security standards.

Date

February 24, 2022

Our reference

[CONFIDENTIAL]

Regulations form a lex specialis, of what is defined as “appropriate” in Article 32 GDPR

measures'.

The AP has considered the scope of the present decision in the following aspects of this article

tested:

- Article 32(2) VIS Regulation prescribes first of all that there must be a security plan to

the confidentiality and integrity of data processing through NVIS

guarantees.

- Member States must take measures to physically protect data, including the

drawing up emergency plans for the protection of critical infrastructure, in accordance with 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 only those authorized to consult the VIS have access

to the data to which their access authorization relates, and exclusively with

personal and unique user identities and secret access procedures (checking 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 within the organization which persons may be eligible for authorisations

Article 32(2)(g) of the VIS Regulation provides an additional safeguard for the use of NVIS

that all authorities with a right of access to the VIS draw up staff profiles detailing the tasks

and responsibilities are defined of the persons authorized to enter data

to view, record, update, delete and search. These profiles must

can be made available to the AP on request and without delay.

- Article 32, second paragraph, under i, 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 are in the VIS when, by whom and for what purpose

incorporated. This means that BZ must keep log files.

Article 32(2)(k) of the VIS Regulation stipulates that the effectiveness of the

security measures is checked and with regard to this internal control the

necessary organizational measures are taken to ensure that the requirements

of this regulation are complied with (checking the log files). This also includes the

security regulations of Article 32 GDPR.

Integrity in processing visa information

Article 28(5) VIS Regulation requires personnel who wish to process data contained in the VIS
stored, first received proper training on data security rules
protection. Only after this training has been received can staff be allowed to work in the VIS
process stored data. This article can be seen as a concrete elaboration of it
principle of integrity, which is laid down in Article 5(1)(f) GDPR. Based on this principle, a
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 ones
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 forms a specialization of what is
laid down in Article 13 GDPR. The AP has assessed whether at the start of the application procedure
a Schengen visa, the obligation to provide adequate information about this to the
person applying for a visa.

This produces the following picture of relevant standards, ranked from general to specific to 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

VIS Vo

Art Art 32 paragraph 2 sub g VIS

Vo.

Logging (internal

check):

Art 32 paragraph 2 sub f, i and k

VIS Vo.

Security incidents

(internal control):

Art 32 paragraph 2 under 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 par. 1(f) (guarantee

up in the organisation

area of integrity and

confidentiality)

Information on

data subjects

Art. 5 Para. 1(a) GDPR

Art. 13 GDPR

Training staff

regarding

data protection:

Art 28 paragraph 5 Vis Vo

Art 38 paragraph 3 Visa Code.

Right to information:

Art. 37 VIS Vo.