Confidential/Registered

Transavia Airlines C.V.

with regard to the management

Piet Guilonardweg 15

1117 EE Schiphol

Date

September 23, 2021

Our reference

[CONFIDENTIAL]

Contact

[CONFIDENTIAL]

Subject

Decision to impose a fine

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

Ir/Madam,

The Dutch Data Protection Authority (AP) has decided to provide Transavia Airlines C.V. an administrative fine of €400,000. The AP has come to the conclusion that Transavia is not a suitable has taken measures to ensure a level of security appropriate to the risk. because of this Transavia has acted contrary to article 32, first and second paragraph, of the General Regulation data protection.

The AP explains the decision in more detail below. Chapter 1 is an introduction and Chapter 2 contains the facts. In Chapter 3, the AP assesses whether personal data is being processed, the

controller and the violation. In chapter 4 the (level of the) administrative

penalty worked out and chapter 5 contains the operative part and the remedy clause.

1

Date

September 23, 2021

Our reference

[CONFIDENTIAL]

1 Introduction

1.1 Organization Involved

This decision concerns Transavia Airlines C.V. (hereinafter: Transavia), located at the Piet Guilonardweg 15, 1117 EE at Schiphol. The company is registered in the trade register under number: 34069081.1 As an airline, Transavia provides flights for business travelers and consumers in Europe.

On October 24, 2019, the AP received a report from Transavia about a security breach of personal data as referred to in Article 33 of the GDPR. Transavia has indicated in this notification that a malicious third party has had unauthorized access to Transavia systems. Nasty as a result of this, the AP has officially investigated whether the technical measures at Transavia met regarding access to personal data were appropriate as referred to in Article 5(1)(f) jo. Article 32 of the GDPR. Specifically, this research focused on access to certain user accounts at Transavia, as well as the rights and possibilities that these user accounts had within the Transavia systems.

1.2 Process flow

On November 28, 2019, the AP contacted Transavia by telephone about the data breach report of October 24, 2019 and subsequent notifications. Then AP supervisors have requested information from Transavia several times, to which Transavia provided this information.

By letter of 12 May 2021, the AP sent Transavia an intention to enforce and the

underlying report with findings. Transavia has this in writing on June 28, 2021

given an opinion.

1 See File document 26, Registration Trade Register Transavia Airlines C.V.

Date

September 23, 2021

Our reference

[CONFIDENTIAL]

2. Facts

2.1 The breach at Transavia

In the data breach notification of October 24, 2019, Transavia indicated that a malicious third party (hereinafter also: 'attacker') has had unauthorized access to Transavia systems.2 Transavia is according to the report found out on October 21, 2019. Transavia then has an external service provider engaged and together with this service provider is the attacker of the systems of Transavia banned. The external service provider also analyzed which systems were affected and what data was involved.

The report drawn up by the external service provider (hereinafter also: 'forensic report') describes that an attacker used [CONFIDENTIAL] email addresses. These addresses are may be found on the Internet.3 The attacker attempted to access the [CONFIDENTIAL]4

The attacker has used a “password spray” or “credential stuffing” attack. With a "password spray” attack, an attacker uses commonly used passwords in an automated manner gain unauthorized access. In a credential stuffing attack, an attacker uses known user data (derived from other third-party data breaches) to attempt to access a system.

At 9:52 AM on September 12, 2019, a successful login attempt was made by the attacker. The

username used was [CONFIDENTIAL] and password was [CONFIDENTIAL]. Of

this login allowed the attacker to use the [CONFIDENTIAL] user.5 This is a user who

was used for [CONFIDENTIAL].6

With the [CONFIDENTIAL] user it was possible to access a Citrix environment from

Transavia. Citrix is software that makes it possible to telework. Then it was possible to

trace possible [CONFIDENTIAL] users in the [CONFIDENTIAL] domain.7

The attacker then succeeded in obtaining the authentication data from the user

[CONFIDENTIAL] by using the password [CONFIDENTIAL] again. This user

2 Transavia France S.A.S. (sister company of Transavia) has reported separately to the French regulator according to the data breach notification of 24 October 2019 because personal data would also be involved where Transavia France S.A.S is responsible for. See File document 1, report dated 24 October 2019.

3 See File document 11, report of 5 December 2019, page 21.

4 Active Directory Federation Services Web service is software from Microsoft that enables organizations to provide Single Sign On Services

achievements in an organization.

5 See File document 11, report of 5 December 2019, page 21.

6 See File document 25, Replies from Transavia, date 26 May 2020.

7 See File document 11, report of December 5, 2019, page 21. A network domain is a group of computers (systems) within a computer network with the aim of centralized management of the systems.

had, according to Transavia, “the highest privileges in the [CONFIDENTIAL]”.8 In principle, this means that the

accounts [CONFIDENTIAL] and [CONFIDENTIAL] together provided access to a large part of

the computer network of Transavia.9 The role of the account was intended to serve as a link between Transavia's HR system and the Active Directory (to determine which employees rights to systems).10 Active Directory is a Microsoft service that (among other things) used to manage user rights.

The attacker then explored Transavia's systems that are part of the domain. In this reconnaissance phase, a login has been made (probably automated) to [CONFIDENTIAL] systems.11 In overall activity has been observed concerning [CONFIDENTIAL] systems. The external service provider has been able to determine on [CONFIDENTIAL] systems that it concerns data that are copied.12 The attacker may have been interested in accessing [CONFIDENTIAL]. Access to this however, it was not successful.13 This was also confirmed by Transavia.14

The attacker has [CONFIDENTIAL] log files on at least [CONFIDENTIAL] systems removed.15

The attacker also used [CONFIDENTIAL] software. This is penetration test software intended to find vulnerabilities in an IT landscape. The external service provider found evidence of this on at least [CONFIDENTIAL] systems. On October 21, 2019 This type of attack has been noticed by the administrator and the administrator has launched an investigation. After October 21 2019, no activity has been observed from the attacker either.16

Based on this alert, Transavia appointed an external service provider on 22 October 2019 enabled (not the administrator). The external service provider has performed a forensic analysis. Out the analysis revealed that the majority of the attacker's activities were aimed at reconnaissance activities. However, the following information was copied: Network documentation, business and various other documents as well as six e-mail boxes.17

Systems have been labeled critical by Transavia [CONFIDENTIAL]. There was a system in between for the exchange of data with [CONFIDENTIAL]. Also included were [CONFIDENTIAL] and a [CONFIDENTIAL]. On one of the critical systems, the [CONFIDENTIAL], certain log files deleted. Because of this, there was less evidence on this system about what happened with this

system.18

8 See File document 38, Replies from Transavia dated 24 September 2020.

9 See File document 11, report of 5 December 2019, page 21.

10 See File document 25, Replies from Transavia, date 26 May 2020.

11 See File document 11, report of 5 December 2019, page 21.

12 See File document 11, report of 5 December 2019, page 26.

13 See File document 11, report of 5 December 2019, page 25.

14 See file document 25, Replies from Transavia, date 26 May 2020.

15 See File document 11, report of 5 December 2019, page 23.

16 See File document 11, report of 5 December 2019, page 25.

17 See File document 11, report of 5 December 2019, page 4.

18 See File document 11, report of 5 December 2019, page 17.

Date

September 23, 2021

Our reference

[CONFIDENTIAL]

On November 22, 2019, Transavia instructed the external service provider to check the mailboxes

studies copied to a remote location by the attacker in this breach. The purpose of

the investigation concerned the personal data in six mailboxes: five mailboxes belonging to employees and one from

a former employee. The mailboxes contained 49 files with personal data.19 These

according to Transavia, mailboxes were (in particular) used by [CONFIDENTIAL] employees.20

These files were then analyzed and on the basis of this it was decided to make a statement to

81,000 data subjects, as required by Article 34 of the GDPR if there may be a high

risk.21 This group of data subjects consisted of Transavia employees and Transavia customers. The

employees whose mailboxes had been copied had already been verbally informed according to

Transavia.22

Transavia indicates that since November 25, 2019, the attacker had definitively no longer had access to the IT landscape of Transavia.23 This has also been confirmed by the external service provider.24

In summary, an unauthorized third party has had access to Transavia systems. Hereby access allowed a user with many privileges to use, giving the attacker a lot capabilities within these systems. Because of this, there has been access to many systems and there are personal data copied to an external location.

2.2 Type of personal data

There are two groups of personal data that can be distinguished in this breach: (1) personal data that the attacker has copied to a remote location and (2) personal data that the attacker has access to had.

2.2.1 Personal Data Copied to an External Location

The following personal data contained in the mailboxes were copied by the attacker (excluding the file names):25

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

19 See File document 25, Replies from Transavia, date 26 May 2020 – Appendix 2: Mailbox investigation report.

20 See File document 25, Replies from Transavia, date 26 May 2020.

21 File document 13, Transavia press release.

22 File document 2, Follow-up report of 22 November 2019.

23 See file document 25, Replies from Transavia, date 26 May 2020.

24 See File document 11, report of 5 December 2019, page 4.

25 File document 25, Replies from Transavia, date 26 May 2020 – Annex 3: Explanation to Annex 2.

Date

September 23, 2021

Our reference

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

The table above shows that passenger, supplier and (potential) employee data

have been copied. Transavia has stated that this concerns approximately 80,000 passengers.26 Also stated in

multiple files containing the personal data of up to 3000 employees and up to 200 suppliers.27

Passengers are involved: first and last name, date of birth, flight information and SSR code. By

one passenger is an address and telephone number involved. The following are the employees

data: first and last name, business e-mail addresses, address, telephone number. And from suppliers

are involved: business e-mail addresses, first and last name, address, e-mail address, telephone number.

26 See file document 25, Replies from Transavia, date 26 May 2020.

27 See File document 25, Replies from Transavia, date 26 May 2020 – Annex 3: Explanation to Annex 2.

Up to 10 CV files of potential employees also appear to be involved. This contained pre-

and surname, address, e-mail address, telephone number and date of birth.

In the notification to the passengers involved (80,000) that Transavia has sent, Transavia reports the

following data involved: first name, last name, date of birth, flight details, booking number

and the additional service such as luggage, but also wheelchair use.28 Transavia also indicates that the

affected employees have also been informed.29

The added services were described as SSR code. SSR code stands for “Special Service Request”

code. Transavia uses a series of 4 characters in their booking system for additional requests, such as

a bicycle as luggage. The SSR code is then “BIKE”.30 These codes can be found on the internet, which means that the meaning is known, if this is not already clear from the code.31

The AP has asked Transavia which SSR codes Transavia uses and in what numbers. The door Codes used by Transavia indicate, among other things, when a wheelchair is required, or whether a passenger use an electric wheelchair, for example. Transavia does not use codes for dietary requirements they do not provide meals during the flights.32

Codes indicating wheelchair use were included in the files that were copied to an external location 358 times before. A code indicating blindness also occurred five times. Deafness occurred four times.33

According to Transavia, the passenger data was collected in the period from 21 to 31 January 2015.34 The data was in a mailbox on “managed devices of employees”.35 These are managed devices, mostly mobile devices such as phones or laptops. The employees in question were [CONFIDENTIAL].

2.2.2 Personal data to which access was possible

Below is an overview of the systems where the users [CONFIDENTIAL] and [CONFIDENTIAL] together.36 The title 'host' in this case means the name of the system. The column “Data seen from / Exfiltrated” indicates whether there are still data after logging into the system other actions have been observed. If "no" is displayed by Transavia, you have only logged in according to Transavia.37

28 See File document 38, Replies from Transavia dated 24 September 2020.

29 See File document 12, Follow-up report of 18 February 2020.

30 See File document 38, Replies from Transavia dated 24 September 2020.

31 See for example: https://wheelchairtravel.org/air-travel/special-service-request-codes/, or https://guides.developer.iata.org/docs/en/list-of-service-ssrs.

32 See File document 38, Replies from Transavia dated 24 September 2020.

33 File document 38, Replies from Transavia date 24 September 2020 - Annex 5: Overview of numbers of SSR codes.

34 See file document 13, Transavia press release.

35 See File document 25, Replies from Transavia, date 26 May 2020.

36 File document 25, Replies from Transavia, date 26 May 2020 – Appendix 4: Host and Personal Data.

37 See File document 25, Replies from Transavia, date 26 May 2020.

Date

September 23, 2021

Our reference

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL].

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

Date

September 23, 2021

Our reference

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL] [CONFIDENTIAL] [CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL] [CONFIDENTIAL] [CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL] [CONFIDENTIAL] [CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL] [CONFIDENTIAL] [CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL] [CONFIDENTIAL] [CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL] [CONFIDENTIAL] [CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL] [CONFIDENTIAL] [CONFIDENTIAL]

Date

September 23, 2021

Our reference

[CONFIDENTIAL]

The tables above show that the following passenger data are processed: the front and surname, date of birth, gender, e-mail address and telephone number, flight and booking details and the (business) e-mail correspondence.

For employees, the first and last name, gender, date of birth, employee number, the home address, telephone number, qualifications/training, citizen service number, attendance records and processed login data. Furthermore, it is mentioned in the overview that reports on a system safety incidents on board. This may also include personal data of employees and passengers involved.

In total, up to 25,000,000 persons involved are listed in the overview provided for passengers. For employees are mentioned up to 3000 people involved. This means that the attacker has personal data has seen or could have seen of 25 million people.

The attacker's level of activity has been broken down by the third-party service provider into the following categories:38

-
-
-
-
-
-

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

On all the systems mentioned there is [CONFIDENTIAL].39 On [CONFIDENTIAL] systems it is actual evidence found for copying personal data. System [CONFIDENTIAL] is regarded as critical by Transavia due to the amount of personal data. On this system there was both mention [CONFIDENTIAL].

On the [CONFIDENTIAL] system, evidence for the attacker's activities was more limited than with other systems, because log files were missing for the relevant period of the infringement.40 Furthermore the system [CONFIDENTIAL] as critical because of the amount of personal data on this system.41 On this system there was mention of [CONFIDENTIAL].

In the report to the AP, Transavia indicated that those involved come from several

countries, namely all of Europe. The AP has requested Transavia has an overview from which country the stakeholders come. Transavia replied that 90% of customers come from the Netherlands, based on the Point of Sale.42 Only a limited number of sister company personal data Transavia France S.A.S. were on the systems of Transavia Airlines C.V. present.43

38 See File document 11, report of 5 December 2019, page 19.

39 See File document 11, report of 5 December 2019, page 32.

40 See File document 11, report of 5 December 2019, page 17.

41 See file document 11, report of 5 December 2019, page 4.

42 See file document 25, Replies from Transavia, date 26 May 2020.

43 See file document 38, Replies from Transavia dated 24 September 2020.

Date

September 23, 2021

Our reference

[CONFIDENTIAL]

The AP comes to the conclusion that Transavia processed personal data of more than 25 million persons. Of these, personal data of up to 83,000 people have been leaked and health data of 367 individuals.

2.3 Security at the Time of the Breach

2.3.1

Transavia's password policy specifies the requirements that apply per user, per option risk level.44 Transavia's password policy states 3 levels:

Access to the [CONFIDENTIAL] domain

“Minimal baseline”, the standard level;

“Medium Additions”, additional measures for users with more privileges;

“Medium and High additions”, additional measures for certain high-risk users.

According to Transavia, the users used by the attacker had the following levels:45

[CONFIDENTIAL] had as level: minimal baseline

[CONFIDENTIAL] had level: Medium and High security additions

The third-party service provider has indicated that the [CONFIDENTIAL] users “contained the highest possible privileges”.

According to the password policy, a minimal baseline user has the following password requirements:46

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

The following additional requirements apply to High security additions:47

□

□

□

□

□

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

44 File document 25, Replies from Transavia, date 26 May 2020 – Appendix 1: Personnel & Access Control Standard.

45 See file document 25, Replies from Transavia, date 26 May 2020.

46 See file document 25, Replies from Transavia, date 26 May 2020 – Appendix 1: Personnel & Access Control Standard.

47 See file document 25, Replies from Transavia, date 26 May 2020 – Appendix 1: Personnel & Access Control Standard.

Date

September 23, 2021

Our reference

[CONFIDENTIAL]

Transavia distinguishes two types of user accounts: “user accounts” and “generic accounts”. The “user accounts” refer to individuals. The “generic accounts” exist for several people or systems, including for links between systems. Logging in to these users is common

automatically place according to Transavia.48

The AP has asked Transavia why the accounts involved in the breach did not comply

to Transavia's own standards. Transavia indicates in its answer that the focus was on “user

accounts” when it comes to password policy compliance. These are relatively more accounts and there

was considered to be the most risky. Transavia has also indicated that this

approach would increase awareness within the organization. Because of this focus, the shortcomings

for the generic accounts involved in the breach have not been noticed.49

The password policy also states that remote access requires multi-factor authentication.50 Off

the report shows that this was not the case for the users that the attacker could access

to acquire. For example, access was made to a Citrix environment without multi-factor authentication. The external

service provider gives as one of the recommendations to Transavia the implementation of

multi-factor authentication for users whose accounts are accessible from the Internet or in any

case for users with many rights.51 Citrix itself also recommends multi-factor authentication for the

use of their application.52

The AP asked Transavia why access was possible to a telework environment without

using multi-factor authentication on the accounts involved in the breach.53

In response, Transavia indicated that the roll-out of

these measures. The implementation of these measures at the “user accounts” took longer than

expected. Flying personnel use applications that are necessary for their work

a safe flight. If a measure such as multi-factor authentication would cause a delay,

this could cause major flight delays. “Generic accounts” had lower priority

Transavia. Because the implementation with the aircrew was delayed, the implementation with the

“generic accounts” also delayed.54

48 See File document 38, Replies from Transavia dated 24 September 2020.

49 See file document 38, Replies from Transavia dated 24 September 2020.

50 See file document 25, Replies from Transavia, date 26 May 2020 – Appendix 1: Personnel & Access Control Standard.

51 See File document 11, report of 5 December 2019, page 21.

52 See file document 40, Citrix best practices, April 9, 2019.

53 File document 30, Letter AP to Transavia dated September 4, 2020.

54 See file document 38, Replies from Transavia dated 24 September 2020.

Date

September 23, 2021

Our reference

[CONFIDENTIAL]

The AP has asked Transavia whether periodic checks take place of the security policy and the actual implementation thereof. Transavia has indicated that there are several periodic checks take place: 55

-
-
-

[CONFIDENTIAL]56

[CONFIDENTIAL]

[CONFIDENTIAL]

The [CONFIDENTIAL] check also indicates that for privileged accounts (accounts with many access rights) there must be a check whether the passwords comply with the policy of Transavia.57 As an example, Transavia provided the results of a [CONFIDENTIAL] audit of 2019, quarter 3. The findings cover the 12-month period before the study. It shows positive and negative results. This is indicated here for several systems the passwords did not comply with Transavia's policy.58

Access within the [CONFIDENTIAL] domain

The AP notes that the passwords used in the attack did not meet the requirements of the

Transavia password policy. There was also no multi-factor authentication for these users,

while these users were accessible via the internet or via telecommuting software.

2.3.2

The attacker had access to virtually the entire [CONFIDENTIAL] domain during the breach. Transavia

has implemented more network segmentation as a follow-up measure.59 According to the National Cyber Security

Center (NCSC), network segmentation is the “dividing the network into functional segments”. Of

network segmentation only separates the systems that need to communicate with each other

segments placed. “Users only get access to the segments they need.”.60

The AP has asked Transavia whether the attacker is using the systems to which automatic access is available

obtained could also have done other things such as copying, viewing or otherwise processing data.61

Transavia has indicated that the attacker had this option.

In the written response, Transavia mentions a number of security measures that were in force on the

moment of the breach: “At the moment of the breach, Transavia had taken various measures in the

as part of its security policy to prevent the consequences of an unauthorized login, including monitoring.

For example, with the Security Operations Center set up for Transavia by its IT supplier, the computers

network activities of Transavia are monitored and checked for anomalous activities. Through this system

55 See file document 38, Replies from Transavia dated 24 September 2020.

56 File document 38, Replies from Transavia dated September 24, 2020 - Annex 6: [CONFIDENTIAL].

57 File document 38, Replies from Transavia dated September 24, 2020 - Annex 6: [CONFIDENTIAL].

58 File document 38, Replies from Transavia date September 24, 2020 - Annex 7: Results [CONFIDENTIAL] 2019 – Q3.

59 See file document 25, Replies from Transavia, date 26 May 2020.

60 See File Document 41, NCSC, Ransomware, Measures to Prevent, Mitigate and Recover from a Ransomware Attack, June

2020.

61 File document 30, Letter AP to Transavia dated September 4, 2020.

Date

September 23, 2021

Our reference

[CONFIDENTIAL]

Transavia received the security notification from its IT supplier on October 21, 2019 indicating unauthorized access to Transavia's IT landscape."62

The forensic report indicated that the administrator had set up logging options, which meant that the external service provider has been able to reconstruct the events to a large extent. The external service provider has been able to use the [CONFIDENTIAL]63 environment of Transavia.64

Research showed that it was possible to delete certain log files. That is indicated log files have been deleted on at least [CONFIDENTIAL] systems for a week. Also is described that certain logging was not maintained in the centralized environment, including from Citrix and certain critical systems. A recommendation from the external service provider is therefore the expand central logging to monitor its integrity. This would also lead to a better response on incidents.65

The forensic report also states that various systems have outdated operating systems were installed. It also says that the implemented multi-factor authentication on certain systems was set up in such a way that a user could enter a telephone number to call a receive second factor message. Certain systems had uncontrolled access to it internet. This allowed the attacker to communicate with remote systems from within the network Transavia.66 Finally, there was insufficient network intruder detection. Because of this there was talk of a limited view of the attacker's network activity.67

2.4 Post-Infringement Measures

After Transavia found out on October 21, 2019 that an attacker has unauthorized access to its systems, Transavia has a forensic analysis performed directly by an external service provider have it executed. After establishing the infringement, Transavia took various measures.

Transavia has introduced two-factor authentication for all end users and devices, among other things.
In addition, the passwords of all user and generic accounts have been reset and are
password requirements technically implemented. Finally, Transavia has divided its network into
multiple segments.68

62 See file document 25, Replies from Transavia, date 26 May 2020.

63 [CONFIDENTIAL] allows data from a large number of different sources to be (automated)
analyze and receive alerts on this. A centralized environment where a system is logging from several
collects, analyzes and reports resources is also referred to as a Security Information and Event Management (SIEM). See
also: File document 42, NCSC, Guidance for implementation of detection solutions, October 2015.

64 See file document 11, report of 5 December 2019, page 4.

65 See File document 11, report of 5 December 2019, pages 23 and 29.

66 See File document 11, report of 5 December 2019, pages 27 and 28.

67 See File document 11, report of 5 December 2019, page 29.

68 Written opinion of Transavia, 28 June 2021, pages 7 and 8.

Date

September 23, 2021

Our reference

[CONFIDENTIAL]

2.5 Transavia's view on the established facts and AP's response

Transavia has nuanced some facts in its view and asked the AP to address these points
pass.69 Insofar as relevant to this decision, the AP briefly mentions this view, accompanied by a
response from the AP.

Transavia would first like to emphasize that the accounts [CONFIDENTIAL] only together (and not each
for themselves) gave access to a large part of Transavia's computer network. And that the overviews
to the data to which the accounts jointly had access. The AP does not dispute this fact. In the

report from the AP described that through access to the first account, the

second account. Nevertheless, the AP has included a further nuance on this in the decision.

Secondly, Transavia states that the exfiltrated data does not mainly consist of contact details

existed. This is in contrast to the files that have only been viewed or could have been viewed by the attacker

see. The historical passenger data file contained no contact details, only before and after

last name, date of birth, flight information and SSR code. The other exfiltrated files contain

do concern business contact details of employees and business contacts, but proportionally

this according to Transavia less data. The AP agrees with Transavia's position and has amended it.

Finally, Transavia indicates that from a passage of the report prepared by the external service provider

it is not so much to read that systems had unnecessary access to the internet, but that these systems

had uncontrolled or unsecured access to it due to the lack of host based firewalls

internet. In response, the AP replaced the word "unnecessary" with "uncontrolled."

69 Written opinion of Transavia, 28 June 2021.

Date

September 23, 2021

Our reference

[CONFIDENTIAL]

3. Review

3.1 Personal Data and Cross-Border Processing

Transavia processes data from passengers, employees and suppliers. Data such as names and

dates of birth are data with which Transavia can identify natural persons. This is possible

directly or indirectly by combining data. Because Transavia processes data with which a

person can be identified directly or indirectly, Transavia processes personal data such as

referred to in Article 4, part 1, of the GDPR.

Transavia also processes personal data relating to wheelchair use, deafness and blindness.

Because this information, along with other linked information, says something about a person's health customer of Transavia, Transavia also processes special categories of personal data as indicated in Article 9 (1) of the GDPR.

Transavia offers services in several European countries. There are also flights to and from several European countries.70 Transavia's passenger data therefore concerns data from those involved several European countries. Transavia has indicated that personal data processed by Transavia are 90% likely to originate from the Netherlands, based on “point of sale”.71 Given the number personal data that Transavia processes from Europeans, the AP still considers 10% to be substantial number.

Because the processing of Transavia from at least one branch involves data subjects from several member states will be, or are likely to be, materially affected, according to the AP concerns cross-border processing as referred to in Article 4, part 23, of the GDPR.

3.2 Controller

In the privacy policy of Transavia Airlines C.V. it has been indicated that Transavia is responsible for the personal data processed by Transavia. Furthermore, Transavia has indicated that the French company is itself responsible for the data that this branch collects.72

Transavia Airlines C.V. has made agreements with sister company Transavia France S.A.S if Transavia France S.A.S uses the systems of Transavia Airlines C.V. through one Service Level Agreement. These agreements state that the management of the ICT systems is the is the responsibility of Transavia Airlines C.V. 73

70 See File document 44, Print website company profile and www.transavia.com.

71 See file document 25, Replies from Transavia, date 26 May 2020.

72 See File document 39, Transavia privacy policy.

73 See File document 38, Replies from Transavia dated 24 September 2020 and appendix 2: Excerpt from SLA Transavia Airlines C.V. – Transavia France S.A.S and appendix 3: Mail Transavia Airlines C.V. to Transavia France S.A.S.

With regard to employee data, Transavia has indicated that this data will be separated processed.74 This means that both the French and Dutch organizations are independently responsible for this data of their own employees. Transavia has provided documentation from which shows that employee data is also stored on systems of Transavia Airlines C.V. are located. 75 Furthermore, Transavia indicated that at the time of the breach only a limited number of systems personal data of Transavia France S.A.S. 76

Transavia Airlines C.V. was also the client for the research by the external party service provider. Transavia Airlines C.V. is also the party informed by the administrator and a has reported the infringement to the AP and those involved.77

In view of the above, Transavia Airlines C.V. the purpose and means of (a large part) of the personal data on the systems as mentioned earlier in chapter 2. The AP has established that Transavia Airlines C.V. the controller is as referred to in Article 4, part 7 of the AVG.

The head office of Transavia Airlines C.V. is also located in Schiphol, the Netherlands.78 In view of the fact established above that Transavia Airlines C.V. as a controller designated, the AP is the lead supervisor. According to Article 56 of the GDPR, the AP has in the European cooperation system IMI consulted with the other supervisors about the fact that the AP sees itself as a leading supervisor. No contradiction has arisen from this procedure other European regulators.

3.3 Appropriate Security Measures

3.3.1

Article 32 of the GDPR contains the requirements regarding the security of the processing of personal data included. The controller must provide appropriate technical and organizational take measures to ensure a level of security appropriate to the risk. When determining appropriate measures should take into account the risk to rights and freedoms of persons.

In the following, the AP tests whether the technical measures at Transavia with regard to access until personal data were appropriate as referred to in Article 32 of the GDPR.

Introduction

74 See File document 38, Replies from Transavia dated 24 September 2020.

75 File document 25, Replies from Transavia, date 26 May 2020 – Appendix 3: Explanation to Appendix 2.

76 See file document 38, Replies from Transavia dated 24 September 2020.

77 See file document 11, report of 5 December 2019, page 4 and file document 1 and 13.

78 See File document 26, Registration Trade Register Transavia Airlines C.V.

Date

September 23, 2021

Our reference

[CONFIDENTIAL]

3.3.2 Assessment

To determine what is appropriate, a trade-off must be made between the state of the art, the implementation costs, as well as the nature, scope, context and processing purposes and qua likelihood and severity of varying risks to the rights and freedoms of individuals. And one up risk-adjusted level of security includes the ability to maintain the confidentiality, integrity, availability and resilience of the processing systems and services guarantee (Article 32 (1) (b) GDPR).

State of the art and implementation costs

As established in Chapter 2, the attacker used a password spray or credential stuffing attack where a hacker applies commonly used or previously leaked passwords. The measures against this can be taken depend, among other things, on the type of application and the possibilities. In this however, the cause of the breach turned out to be a simple and commonly used password in two users that was easy (automated) to guess. The strength and level of the password was not in accordance with Transavia's own authentication policy.

It is certain that Transavia has a policy for user authentication. It is also established that Transavia carries out periodic checks and continuously works on its own security policy. From the door However, periodic security checks supplied by Transavia show that many applications do not the password policy of Transavia itself was complied with.

Transavia has indicated that the generic accounts used during the breach are not the focus during internal audits. For example, the passwords of generic accounts have not been verified were used according to its own policy. According to Transavia, the risk lay with other types of accounts, namely, the user accounts linked to individual users. This is why the bad ones passwords not noticed in time according to Transavia. It is also indicated that multi-factor authentication implement for “generic accounts” had not yet been realized at the time of the breach, because implementation to other users was delayed.

After the first successful authentication, a Citrix environment was used. This environment is then used by the attacker to gain further access to Transavia's systems.

For these types of environments, it is recommended to use multi-factor authentication to gain access to limit. As mentioned earlier, this is a common measure that was also used at the time of the breach was advised by the provider of the teleworking software Citrix.

After the attacker gained further access, he/she had many freedoms on the systems of Transavia. Ultimately, this resulted in the copying of personal data from mailboxes staff. This could have been prevented by dividing the network into several segments.

Furthermore, the rights of users can be adjusted to determine whether they are necessary

users have these rights (authorisations). Transavia has this measure after the infringement

implemented.

It also turned out to be possible to save log files on systems that have been designated as critical by Transavia

to delete. As a result, after the breach, there was no complete picture of what had happened on these systems.

Commonly used information security standards that were valid at the time of the

violate password management, network segmentation, and user rights

various recommendations. For example, as a control measure, safeguarding strong

passwords. Groups of information systems must also be separated into networks. Further

indicates that access rights must be restricted and controlled and must be accessed

information to be limited. 79

The measures that Transavia could have taken at the time of the infringement already complied with a standard

Transavia itself, according to suppliers and according to international standards. Furthermore, it turned out that there were

certain

measures had already been partly implemented by Transavia.

Based on the above, the AP is of the opinion that, given the state of the art at the time of the

breach, it was certainly possible to implement security measures for the risk that arises

realized in the infringement. The introduction of the essential precautions mentioned above

would have made it possible to maintain the confidentiality of the personal data processed

in accordance with Article 32 (1) (b) of the GDPR and the risk of the occurrence of the

substantially reduce data breaches.

The information supplied by Transavia also shows that after the breach a multiple of

measures have been taken including changing passwords, implementing

network segmentation and adjusting user rights. The AP considers the implementation costs for this

security measures not so high that these measures could not be implemented earlier

become.

The nature, scope, context and processing purposes

For example, as the data is processed on a large scale and becomes more sensitive,

stricter requirements are imposed on the security of the data.

The AP has established that Transavia processes a large amount of personal data, including

special personal data such as health data. The attacker had access to systems where

contains records of approximately 25 million passengers. Given this large-scale processing of

personal data, the AP does not consider Transavia's security to be adequate at the time of the breach.

Probability and severity of varying risks to the rights and freedoms of individuals

The breach involved unauthorized access and provision of personal data.

Furthermore, not only could the attacker have had access to much more personal data, it was

possible to copy or otherwise process this data. The data processed by Transavia

such as contact details, in the hands of a malicious third party can be misused for

purposes that may lead to material or immaterial damage.80 Transavia also processes

79 See file document 43: NEN-norm_ISO_27001_2017_nl, pages 23, 24 and 29.

80 For example, contact details can be used by a malicious third party for phishing. Phishing is aimed at getting

(sensitive) information, in order to commit fraud. See also: https://www.ncsc.nl/onderwerpen/phishing.

special personal data of passengers and BSN numbers of employees. A breach of the

confidentiality of this can lead to immaterial damage, such as discrimination or fraud.81

Appropriate technical measures

In view of the above, the AP is of the opinion that the technical measures were not 'appropriate' at the time of the infringement, as referred to in Article 32 of the GDPR. Considering the quantity and type personal data processed by Transavia, a high level of measures must be taken. A breach of the confidentiality of this data can be material or result in immaterial damage.

The measures that Transavia could have taken were possible and appropriate given the state of the technology and implementation costs. The lack of these measures, on multiple levels, has led to a (realized) risk to the rights and freedoms of data subjects.

3.3.3 Transavia's view and AP's response

Below, the AP briefly summarizes Transavia's view on the AP's assessment, provided of a response from the AP.

View Transavia

In its opinion, Transavia indicates that it has embedded a continuous improvement process cyclically its organization according to the standardization and Plan-Do-Check-Act cycle generally used in the sector (PDCA). Against this background, Transavia has implemented a user authentication policy (the 'Authentication Policy') established in December 2017 with a policy horizon of three years ('Plan' phase). Transavia realizes that the passwords of the compromised accounts in 2019 did not meet the own Authentication Policy. Although the Authentication Policy was appropriate according to Transavia itself, such as referred to in Article 32 GDPR, the implementation of that policy was not complete. The passwords of the compromised accounts did not comply with its own policies and as such were not appropriate for it intended level of security.

However, Transavia wants the AP's image in the research report on multi-factor authentication nuance. Based on the information available at the time, Transavia expected that the chance of a successful password spray attack or credential stuffing attack was greater for user accounts than for

generic accounts. User account information is generally much easier to find

on the internet (think of the name of the person in combination with the organization, data on Linkedin), then

information about generic accounts that are not linked to an individual. In addition, this one played

consideration for Transavia an important role that the number of user accounts in proportion many times

was greater than the number of generic accounts. Transavia wants to emphasize that they have the choice to prioritize

give to user accounts has carefully taken into account at that time

81 See also: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/security/notify-data-leaks#when-delivers-a-data-leak-a-high-risk-on-7331.

foreseeable risks. Finally, Transavia would like to point out that, with regard to the introduction of multi-factor authentication between 2017 and 2019, kept pace with the rest of the industry.

Reply AP

The AP has established that the security measures at several levels are insufficiently appropriate

goods. The combination of weak passwords and the lack of two-factor authentication

made it foreseeable, according to the AP, that there was a high risk of unauthorized access to the

personal data of Transavia. Two-factor authentication has been common for many years

security measure and quite easy to implement. The AP sees on the basis of the nuance of

Transavia about multi-factor authentication is no reason to adjust the assessment in this regard.

3.4 Conclusion

The AP comes to the conclusion that Transavia did not take appropriate measures at the time of the infringement

to ensure a level of security appropriate to the risk. This has put Transavia in conflict

acted in accordance with Article 32, first and second paragraph, of the GDPR.

Date

September 23, 2021

Our reference

[CONFIDENTIAL]

4. Fine

4.1 Introduction

Transavia has acted in violation of article 32, first and second paragraph, of the GDPR. The AP makes for the established violation will use its authority to impose a fine on Transavia. Seen the seriousness of the violation and the extent to which this can be attributed to Transavia, the AP deems the imposition of a fine. The AP motivates this in the following.

4.2 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 notify Transavia in the event of a to impose an administrative fine of up to € 10,000,000 or, for a violation of Article 32 of the GDPR, company, up to 2% of the total worldwide annual turnover in the previous financial year, if this figure is higher.

The AP has established Fining Policy Rules regarding the implementation of the aforementioned power to imposing an administrative fine, including determining the amount thereof.82 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.

4.3 Fine amount

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.

4.3.1 Severity of the Violation

The AP has come to the conclusion that Transavia has not applied an appropriate security level for the processing of personal data in its network. Transavia processes many types of personal data, such as contact details of passengers and the citizen service number, attendance records and login details its employees. Transavia also processes health data, such as wheelchair use, deafness and blindness of passengers.

It is also important that Transavia processed personal data of more than 25 at the time of the breach million persons. At the time, Transavia involved the personal data of this large group of data subjects

82 Stct. 2019, 14586, March 14, 2019.

insufficiently secured. This huge group of citizens have run an unnecessary extra risk of, among other things unauthorized access to their personal data. A risk that has incidentally been realized by the breach from 2019 leaking personal data of up to 83,000 individuals and health data of 367 persons.

Due to the fact that data processing is extensive in this violation, it is a large number concerns data subjects and special personal data were also processed, the AP qualifies these breach of the GDPR as very serious.

In view of the above, the AP sees reason to, based on the degree of seriousness of the violation to impose a fine on Transavia and to increase the (basic) amount of the fine to € 400,000.

4.3.2 Culpability, negligence and mitigation measures

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. In addition, the AP also takes into account the negligent nature of the infringement and the damage-limiting measures by Transavia.

Under Article 32 of the GDPR, Transavia is obliged to introduce security measures that are appropriate for the nature and scope of the processing carried out by Transavia. Considering the (sensitive) nature and the large scope of the processing, the AP is of the opinion that Transavia is in any case special has been negligent in taking such measures sufficiently. May be from Transavia expects it to ascertain the standards that apply to it and to act accordingly. The AP considers this culpable.

In addition, the AP has determined that the periodic security checks supplied by Transavia it turned out that many applications did not comply with Transavia's own password policy.

The AP considers it very negligent that Transavia did not immediately take action to prevent such a to ensure an appropriate level of security. On the other hand, Transavia has after taking note of it data breach, many measures were immediately taken to protect personal data more appropriately and to prevent the attacker from accessing Transavia's systems any longer. In addition, has Transavia indicated that it has also generally taken several measures to reduce the security level in the company.

In view of the above considerations, the AP therefore sees reason to set the fine on the basis of the negligent nature of the infringement by € 25,000. But also for the amount of the fine under the reduce the damage-limiting measures taken by € 25,000.

4.3.3 Other Circumstances

In its opinion, Transavia states that the parties involved are almost certain to have no
have been adversely affected by the data breach. The leaked passenger data contained none
contact details and were not or only to a limited extent sensitive. Transavia has had none for the past year and a half
reported misuse of data. Transavia also reported the data leak to the AP in good time
and informed those involved. Finally, Transavia cooperated as well as possible with the investigation
of the AP and no profits were made or losses avoided from the breach.

The AP is of the opinion that Transavia's cooperation has not gone beyond its legal obligation
to comply with Article 31 of the GDPR. Transavia has not cooperated in any particular way with this
with the AP. Also the circumstance that Transavia only complies with its legal obligation to report to the AP
and those involved, given the seriousness of this violation, the fulfillment of this obligation cannot be regarded as a
mitigating or mitigating factor. Finally, the AP notes that the right of
the protection of personal data of various data subjects has indeed been damaged, because
for example, passenger health data and employee contact details
came from a malicious third party. These persons involved are prevented from retaining the
control of their personal data.

Given the seriousness of the violations and the degree of culpability, the AP does not express this view
reason to waive the imposition of a fine or to waive the fine on the grounds stated by Transavia
moderate.

4.3.4 Proportionality

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 fine in view of the circumstances of the specific case, not one
disproportionate outcome.

The AP is of the opinion that (the amount of) the fine is proportionate.83 In this opinion, the AP has assessed the seriousness
of the

violation, the extent to which this can be blamed on Transavia, the damage-limiting measures

and other circumstances taken into account. Due to the large volume of data processing, the fact

that it concerns a large number of data subjects and that special personal data were also processed

the AP qualifies this breach of the GDPR as very serious.

Given all the circumstances of this case, the AP sees no reason to set the amount of the fine on the grounds of

the proportionality and the circumstances referred to in the Fining Policy Rules, insofar as applicable

the present case, to increase or decrease even further.

4.4 Conclusion

The AP sets the total fine amount at € 400,000.

83 For the justification, see sections 4.3.1 and 4.3.2.

Date

September 23, 2021

Our reference

[CONFIDENTIAL]

5. Operative part

The AP explains to Transavia Airlines C.V. due to violation of article 32, first and second paragraph, of the AVG

an administrative fine in the amount of:

€ 400,000 (say four hundred thousand euros).84

Yours faithfully,

Authority for Personal Data,

e.g.

drs. C.E. Mur

Board member

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. Submit it

of a notice of objection suspends the effect of this decision. For submitting a digital objection, see

www.autoriteitpersoonsgegevens.nl, under the heading 'Make an objection', at the bottom of the page under the heading

"Contact with the Dutch Data Protection Authority". The address for paper submission is: Authority

Personal data, PO Box 93374, 2509 AJ The Hague. Mention 'Awb objection' on the envelope and put in the

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

 Your name and address

 The date of your objection

 The reference mentioned in this letter (case number); you can also get a copy of this decision

attach

 The reason(s) why you disagree with this decision

 Your signature

For more information, see: https://autoriteitpersoonsgegevens.nl/nl/bezwaar-maken

84 The AP will hand over the aforementioned claim to the Central Judicial Collection Agency (CJIB).