Confidential/Registered

Transavia Airlines CV

to the board of directors

Piet Guilonardweg 15

1117 EE Schiphol

Date

September 23, 2021

Our reference

[CONFIDENTIAL]

Contact

[CONFIDENTIAL]

Topic

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

authority data.nl

Dear Sir / Madam,

The Dutch Data Protection Authority (AP) has decided to grant Transavia Airlines C.V. an administrative fine

of €400,000. The AP has come to the conclusion that Transavia is not an appropriate

has taken measures to ensure a level of security appropriate to the risk. because of this

has Transavia acted in violation of 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 DPA assesses whether personal data is being processed, the

processing responsibility and the violation. In chapter 4 the (height of the) administrative fine and Chapter 5 contains the operative part and the remedies clause.

1

Date

September 23, 2021

Our reference

[CONFIDENTIAL]

1 Introduction

1.1 Organization involved

This decision relates to Transavia Airlines C.V. (hereinafter: Transavia), located at the Piet Guilonardweg 15, 1117 EE, 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. In this notification, Transavia has indicated that a malicious third party has had unauthorized access to Transavia systems. Unpleasant As a result, the AP has officially investigated whether the technical measures at Transavia with regard to 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 systems of Transavia.

1.2 Process

On November 28, 2019, the AP contacted Transavia by telephone about the data breach report of 24 October 2019 and subsequent notifications. Supervisors of the AP subsequently requested information from Transavia several times on which Transavia has provided this information.

In a letter dated 12 May 2021, the AP sent Transavia an intention to enforce and

the underlying report with findings. Transavia has written to this effect on 28 June 2021

given an opinion.

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

Date

September 23, 2021

Our reference

[CONFIDENTIAL]

2. Facts

2.1 The infringement at Transavia

In the data breach notification of 24 October 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 subsequently has an external

service provider and together with this service provider is the attacker of the systems of

Transavia banned. Furthermore, the external service provider 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 has used [CONFIDENTIAL] email addresses. These addresses are

may be found on the Internet.3 The attacker attempted to access the

[CONFIDENTIAL]4

The attacker used a “password spray” or “credential stuffing” attack. With a "password

spray” attack, an attacker uses commonly used passwords to automate

gain unauthorized access. In a “credential stuffing” attack, an attacker uses known

user data (from other third-party data breaches) to attempt to access

a system.

A successful login attempt by the attacker took place on September 12, 2019 at 9:52 AM. 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 telecommute. It was then possible to

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

The attacker was then able to obtain the user's authentication information

[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 1, notification of 24 October 2019.

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

4 Active Directory Federation Services Webservice is software from Microsoft that enables organizations to use Single Sign On Services

achievements in an organization.

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

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

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

Date

September 23, 2021

Our reference

[CONFIDENTIAL]

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

[CONFIDENTIAL] and [CONFIDENTIAL] accounts together provided access to much of

Transavia's computer network.9 The account's role 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)
is used to manage user rights.
The attacker then explored Transavia's systems that are part of the domain. In this
reconnaissance phase, has (probably automated) logged into [CONFIDENTIAL] systems.11 In
in total, activity has been observed concerning [CONFIDENTIAL] systems. The external service provider
has been able to establish on [CONFIDENTIAL] systems that there is data that is
copied.12 The attacker may have been interested in accessing [CONFIDENTIAL]. Access to this
however, it was not successful.13 This has also been confirmed by Transavia.14
The attacker has [CONFIDENTIAL] log files on at least [CONFIDENTIAL] systems
deleted.15
The attacker has also made use of [CONFIDENTIAL] software. This is penetration test
software intended to find vulnerabilities in an IT landscape. The external service provider
has found indications for this on at least [CONFIDENTIAL] systems. On October 21, 2019
This type of attack was noticed by the administrator and the administrator has investigated. After October 21
In 2019, no more activities were observed from the attacker.16
On the basis of this signal, Transavia established an external service provider on October 22, 2019.
enabled (not the administrator). The external service provider has performed a forensic analysis. Out
the analysis found that the majority of the attacker's activities focused on
reconnaissance activities. However, the following data has been copied: Network documentation,
business and various other documents as well as six e-mail boxes.17
Systems have been labeled as 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 to this

system.18

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

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

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

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

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

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

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

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

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

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

18 See File 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 open the mailboxes

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

the investigation concerned the personal data in six mailboxes: five employee mailboxes and one of

a former employee. 49 files with personal data were found in the mailboxes.19 These

According to Transavia, mailboxes were (mainly) 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 is a possible high

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

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

Transavia.22

Transavia indicates that since November 25, 2019, the attacker 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, it was possible to use a user with many privileges, giving the attacker a lot of capabilities within these systems. As a result, there has been access to many systems and there are also personal data copied to an external location.

2.2 Type of personal data

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

2.2.1 Personal data copied to a remote location

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

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

19 See File 25, Replies from Transavia, date 26 May 2020 – Appendix 2: Investigation report mailboxes.

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

21 File 13, Transavia Press Release.

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

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

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

25 File 25, Replies from Transavia, date 26 May 2020 – Appendix 3: Explanatory notes to Appendix 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

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

From passengers are concerned: first and last name, date of birth, flight information and SSR code. From

one passenger is an address and phone number involved. From employees it is about the following

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

are involved: business email addresses, first and last name, address, email address, telephone number.

26 See File 25, Answers from Transavia, date 26 May 2020.

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

Date

September 23, 2021

Our reference

[CONFIDENTIAL]

It also appears that up to 10 CV files of potential employees are involved. This included pre-

and last name, address, email address, telephone number and date of birth.

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

following data concerned: 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 states that the

involved employees are also informed.29

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

code. Transavia uses a 4-character string 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 e.g. use an electric wheelchair. Transavia does not use codes for dietary requirements as they do not provide meals during the flights.32

The files copied to an external location contained codes indicating wheelchair use 358 times before. Also, a code indicating blindness 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 located in a mailbox on “employee managed devices”.35 These are managed devices devices, mostly mobile devices such as telephones 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] had access to them together.36 The title ‘host’ in this case means the name of the system. The column “Data viewed from /Exfiltrated” indicates whether there is still information after logging into the system other actions have been observed. If "no" is displayed by Transavia, there is only logged in according to Transavia.37

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

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

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

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

34 See File 13, Transavia Press Release.

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

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

37 See File 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]

It appears from the above tables that the following data is processed for passengers: the front and surname, date of birth, gender, e-mail address and telephone number, flight and booking details and the (business) e-mail correspondence.

Employees' first and last name, gender, date of birth, employee number, the home address, telephone number, qualifications/training, citizen service number, attendance administration and login details processed. Furthermore, it is stated in the overview that reports about safety incidents on board. This may also contain personal data of employees and passengers involved.

In total, up to 25,000,000 persons involved are mentioned in the supplied overview for passengers. In front of employees are mentioned up to 3000 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 mentioned systems there is talk of [CONFIDENTIAL].39 On [CONFIDENTIAL] systems there is actual evidence found for copying personal data. System [CONFIDENTIAL] is considered critical by Transavia due to the amount of personal data. On this system there was both refer to [CONFIDENTIAL].

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

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

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

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

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

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

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

43 See File 38, Replies from Transavia date September 24, 2020.

Date

September 23, 2021

Our reference

[CONFIDENTIAL]

The AP comes to the conclusion that at the time of the infringement, Transavia was processing 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 states which requirements apply per user, per possible risk level.44 Transavia's password policy states 3 levels:

Access to the [CONFIDENTIAL] domain

“Minimal baseline”, the default level;

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

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

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

[CONFIDENTIAL] was level: minimal baseline

[CONFIDENTIAL] had level: Medium and High security additions

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

A user with minimal baseline has the following password requirements according to the password policy:46

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

The following additional requirements apply for High security additions:47

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

[CONFIDENTIAL]

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

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

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

47 See File 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” concern individuals. The “generic accounts” exist for several people or

systems, including for links between systems. Logging in to these users often finds

automatically place according to Transavia.48

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

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

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

it was considered that most of the risks would arise from this. 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 infringement 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

as one of the recommendations to Transavia, the service provider recommends implementing

multi-factor authentication for users whose accounts can be accessed from the internet or in any

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

use their application.52

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

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

In response, Transavia has 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 multiple factors would cause authentication delay,

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

Transavia. Because the implementation among the aircrew was delayed, the implementation at the

“generic accounts” also delayed.54

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

49 See File 38, Replies from Transavia date 24 September 2020.

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

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

52 See File 40, Citrix best practices, April 9, 2019.

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

54 See File 38, Replies from Transavia date September 24, 2020.

Date

September 23, 2021

Our reference

[CONFIDENTIAL]

The AP has asked Transavia whether periodic checks were made 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) check whether the passwords comply with the policy of Transavia.57 As an example of this, Transavia has provided the results of a [CONFIDENTIAL] 2019 quarter 3 audit. The findings cover the 12-month period prior to the study.

This shows positive and negative results. For several systems it is indicated here that the passwords did not comply with Transavia's policy.58

Access within the [CONFIDENTIAL] domain

The AP determines that the passwords used in the attack did not meet the requirements of the password policy of Transavia. Also, for these users no multi-factor authentication was present, while these users were accessible via the internet or via telework 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 network into functional segments”. Of network segmentation, only the systems that need to communicate with each other are put together in separate segments placed. “Users only get access to the segments they need.”.60

The AP has asked Transavia whether the attacker can access the systems to which there is automatic access obtained could also have done other things such as copying, viewing or otherwise editing data.61 Transavia has indicated that the attacker had this option.

In its written response, Transavia mentions a number of security measures that were in force on the time of the infringement: “At the time of the infringement, Transavia had taken various measures in the as part of its security policy to prevent the consequences of an unauthorized login attempt, including monitoring. For example, with the Security Operations Center set up for Transavia by its IT supplier, the computer and network activities of Transavia and checked for abnormal activities. Through this system

55 See File 38, Replies from Transavia date September 24, 2020.

56 File 38, Replies from Transavia date September 24, 2020 - Appendix 6: [CONFIDENTIAL].

57 File 38, Replies from Transavia date September 24, 2020 - Appendix 6: [CONFIDENTIAL].

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

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

60 See File 41, NCSC, Ransomware, measures to prevent, mitigate and recover from a ransomware attack, June 2020.

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

[CONFIDENTIAL]

On October 21, 2019, Transavia received the security notification from its IT supplier that indicated unauthorized access to the IT landscape of Transavia."62

It was indicated in the forensic report that the administrator had set up logging options, so 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. It is indicated that 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 extend central logging to monitor its integrity. This would also lead to a better response on incidents.65

The forensic report also states that outdated operating systems were installed. It also states that the implemented multi-factor authentication on certain systems had been set up in such a way that a user could enter a telephone number himself to to receive a second factor message. Certain systems had uncontrolled access to the internet. This allowed the attacker to communicate with remote systems from the network of Transavia.66 Finally, there was insufficient network intruder detection. As a result, there was from 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 had a forensic analysis performed directly by an external service provider have it carried out. After the infringement was established, 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 25, Replies from Transavia, date 26 May 2020.

63 [CONFIDENTIAL] makes it possible to (automatically) collect data from a wide variety of sources

analyze and receive alerts on this. A centralized environment where a system logs from different

collects, analyzes and reports sources is also called a Security Information and Event Management (SIEM). See

also: Dossierstuk 42, NCSC, Guidance for the implementation of detection solutions, October 2015.

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

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

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

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

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

Date

September 23, 2021

Our reference

[CONFIDENTIAL]

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

Transavia has nuanced some facts in its view and asked the AP to add these points

69 Insofar as it is relevant to this decision, the DPA briefly mentions this view, accompanied by a

response from the AP.

First of all, Transavia would like to emphasize that the accounts [CONFIDENTIAL] only together (and not each

themselves) gave access to a large part of Transavia's computer network. And that the overviews

view the data that the accounts had joint access to. The AP does not dispute this fact. In the

report from the AP describes that access to the first account has been gained to 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 consist mainly of contact details existed. This is in contrast to the files that were only seen or could have been viewed by the attacker see. The historical passenger data file contained no contact details, only front and surname, date of birth, flight information and SSR code. The other exfiltrated files contain are business contact details of employees and business contacts, but are proportionate according to Transavia, this is less data. The AP agrees with this position of Transavia and has adjusted 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 unnecessarily access to the internet, but that these systems due to the lack of host based firewalls had uncontrolled or unsecured access to the internet. In response, the AP has replaced the word “unnecessary” with “unsupervised.”

69 Written opinion Transavia, 28 June 2021.

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(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 the health of a 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 is also flown to and from several European countries.70 Transavia's passenger data therefore concerns data from data subjects from several European countries. Transavia has indicated that personal data processed by Transavia 90% probably come from the Netherlands, based on “point of sale”.71 In view of the number personal data that Transavia processes from Europeans, the AP still considers 10% a substantial number of.

Because in the processing of Transavia from at least one branch, data subjects from several Member States will be, or are likely to be, materially affected, according to the AP refers to 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 responsible for the data that this branch collects.72

Transavia Airlines CV 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 a Service Level Agreement. These agreements state that the management of the ICT systems is the responsibility of Transavia Airlines C.V. 73

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

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

72 See File 39, Transavia privacy policy.

73 See File 38, Replies from Transavia dated September 24, 2020 and Appendix 2: Fragment from SLA Transavia Airlines C.V. –

Transavia France S.A.S and Annex 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 segregated

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

it appears that employee data is also stored on systems of Transavia Airlines C.V. located. 75

Furthermore, Transavia has indicated that at the time of the infringement only a limited number of systems

personal data of Transavia France S.A.S. 76

Transavia Airlines CV was also the client for the research by the external

service provider. Transavia Airlines CV 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. determine the purpose and means of (a large part of)

of the personal data on the systems as mentioned earlier in chapter 2. The DPA establishes that

Transavia Airlines CV the controller is as referred to in Article 4, part 7 of the

GDPR.

The headquarters of Transavia Airlines C.V. is also located in Schiphol, the Netherlands.78 In view of the

fact that it has been established above that Transavia Airlines C.V. as a data controller can become

designated, the AP is the lead supervisory authority. According to Article 56 of the GDPR, the AP has in the

European cooperation system IMI consulted with the other regulators about the fact that the AP

sees itself as a leading regulator. No contradiction has arisen from this procedure from

other European regulators.

3.3 Appropriate security measures

3.3.1

Article 32 of the GDPR sets out the requirements for the security of the processing of personal data

Hospitalized. 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 checks 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 38, Replies from Transavia date 24 September 2020.

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

76 See File 38, Replies from Transavia date 24 September 2020.

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

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

Date

September 23, 2021

Our reference

[CONFIDENTIAL]

3.3.2 Assessment

In order to determine what is appropriate, a trade-off must be made between the state of the art, the execution costs, as well as the nature, scope, context and processing purposes and qua probability and severity differing risks to the rights and freedoms of individuals. And one on risk-adjusted security level includes the ability to confidentiality, integrity, availability and resilience of the processing systems and services guarantee (Article 32(1)(b) of the 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
breach, however, the cause of the breach turned out to be a simple and commonly used password at 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 established that Transavia has a policy for user authentication. It is also established that Transavia
conducts periodic audits and continuously works on its own security policy. Out of the door
Periodic security checks supplied to Transavia, however, show that in many applications there is no
Transavia's own password policy was complied with.
Transavia has indicated that the generic accounts used during the infringement are not the focus
had during internal audits. For example, it has not been checked whether the passwords of generic accounts
were used according to their own policy. According to Transavia, the risk lay with other types of accounts,
namely the user accounts associated with individual users. As a result, the bad
passwords were not detected in time according to Transavia. Furthermore, it has been indicated that multi-factor authentication
implementing for “generic accounts” had not yet been realized at the time of the breach, because
the implementation with other users had been 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 access
to limit. As mentioned earlier, this is a common measure that was also taken at the time of the infringement
was advised by the provider of the telecommuting 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 of
Staff members. This could have been prevented by dividing the network into several segments.
Furthermore, the rights of users can be adjusted, to determine whether it is necessary that these
users have these rights (authorizations). Transavia has taken this measure after the infringement
implemented.

It also turned out to be possible to store log files on systems that have been identified as critical by Transavia remove. As a result, there was no complete picture of what had happened on these systems after the breach.

Commonly used information security standards that were valid at the time of the violating password management, network segmentation and user rights different recommendations. For example, as a control measure, the safeguarding of strong passwords. Groups of information systems in networks must also be separated. Further indicates that access rights should be restricted and controlled and access to information to be limited. 79

The measures that Transavia could have taken at the time of the infringement were already a standard according to Transavia itself, according to suppliers and according to international standards. Furthermore, it was found that certain measures had already been partly implemented by Transavia.

Based on the above, the AP is of the opinion that, in view of the state of the art at the time of the breach, it was certainly possible to implement security measures for the risk that realized in the infringement. The introduction of the above-mentioned essential precautions 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 to substantially reduce data leakage.

It also appears from the information supplied by Transavia that after the infringement 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 purposes of processing

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 data on approximately 25 million passengers. Given this large-scale processing of

personal data, the AP considers the security of Transavia to be inadequate at the time of the breach.

Likelihood and severity of varying risks to individuals' rights and freedoms

The breach involved unauthorized access and disclosure of personal data.

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

possible to copy or otherwise process this data. The data that Transavia processes,

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

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

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

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

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

special personal data of passengers and social security numbers of employees. An infringement of the

their confidentiality 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. Given the amount and type personal data that Transavia processes, 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 several levels, has led to a (realised) risk to the rights and freedoms of data subjects.

3.3.3 Transavia's view and AP . response

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

Transavia's view

In its view, Transavia indicates that it has embedded a continuous improvement process cyclically in its organization according to the standards generally applied in the sector and the Plan-Do-Check-Act cycle (PDCA). Against this background, Transavia has adopted a policy for user authentication (the 'Authentication Policy') established in December 2017 with a three-year policy horizon (phase 'Plan').

Transavia realizes that the passwords of the compromised accounts in 2019 did not comply with the own Authentication Policy. Although the Authentication Policy itself was appropriate according to Transavia, 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 policy and in that sense were not appropriate for the intended level of security.

However, Transavia wants the image of the AP 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 on user accounts than on generic accounts. User account data is generally much easier to find on the internet (think of person's name in combination with the organization, data on Linkedin), then data about generic accounts that are not linked to a person. In addition, this

consideration for Transavia an important role that the number of user accounts is many times over

was greater than the number of generic accounts. Transavia would like to emphasize that it has made the choice to prioritize

giving to user accounts carefully, taking into account the then

81 See also: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/veiligheid/meldplicht-datalek#wanneer-levert-een-datalek-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.

Response AP

The AP has found 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 years

security measure and quite easy to implement. On the basis of the nuance of ., the AP sees

Transavia about multi-factor authentication is not a reason to adjust its assessment.

3.4 Conclusion

The AP concludes that Transavia did not take appropriate measures at the time of the infringement

to ensure a level of security appropriate to the risk. As a result, Transavia has

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

Our reference

[CONFIDENTIAL]

4. Fine

4.1 Introduction

Transavia has acted in violation of Article 32(1) and (2) of the GDPR. The AP makes for the established violation uses its power to impose a fine on Transavia. Seen the seriousness of the violation and the extent to which it can be blamed on Transavia, the AP deems the imposition of a fine. The AP justifies this in the following.

4.2 Fine policy rules of the Dutch Data Protection Authority 2019

Pursuant to Article 58, second paragraph, preamble and under i and Article 83, fourth paragraph, of the GDPR, read in In connection with Article 14, third paragraph, of the UAVG, the AP is authorized to grant Transavia in the event of a violation of Article 32 of the GDPR to impose an administrative fine of up to € 10,000,000 or, for a company, up to 2% of the total worldwide annual turnover in the previous financial year, if this figure is higher.

The AP has established fine policy rules regarding the interpretation of the aforementioned power to imposing an administrative fine, including determining the amount thereof.82 In the Fines policy rules have been chosen for a category classification and bandwidth system.

Violation of Article 32 of the GDPR is classified in Category II. Category II has a fine range 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 decreasing or increasing the base amount. It is an assessment of the seriousness of the violation in the specific case, the extent to which the violation can be attributed to the offender be blamed and, if there is reason to do so, other circumstances.

4.3.1 Seriousness 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, the attendance administration and login details of
its employees. Transavia also processes health data, such as wheelchair use,
deafness and blindness of passengers.
In addition, it is important that Transavia was processing personal data of more than 25 % at the time of the infringement
million people. At the time, Transavia had the personal data of this large group of data subjects
82 Stct. 2019, 14586, March 14, 2019.

Date
September 23, 2021
Our reference
[CONFIDENTIAL]
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 was realized by the infringement
from 2019 leaking personal data of up to 83,000 people and health data of 367
persons.
Due to the fact that the data processing is extensive in this violation, a large number of
concerned and special personal data were also processed, the AP qualifies these
breach of the GDPR as very serious.
In view of the above, based on the degree of seriousness of the violation, the AP sees reason to
impose a fine on Transavia and increase the (basic) amount of the fine to € 400,000.
4.3.2 Liability, negligence and mitigation measures
Pursuant to Article 5:46, second paragraph, of the Awb, when imposing an administrative fine, the AP
into account the extent to which this can be blamed on the offender. Now that this is a
violation, the imposition of an administrative fine in accordance with established case law does not require that
it is demonstrated that there is intent and the AP may presume culpability if it

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

Transavia is obliged under Article 32 of the GDPR to implement security measures that are appropriate for the nature and scope of the processing operations that Transavia carries out. In view of the (sensitive) nature and the large scale of the processing, the DPA is of the opinion that Transavia is in any case particularly has been negligent in taking such measures adequately. May be from Transavia expects it to ascertain and act upon the standards that apply to it. The AP considers this blameworthy.

In addition, the AP has established that from the periodic security checks provided 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 after these checks to appropriate level of security. On the other hand, after becoming aware of the data breach immediately took many measures to protect personal data more appropriately and to prevent the attacker from entering Transavia's systems any longer. In addition, Transavia indicated that it has also generally taken several measures to increase the level of security in the company.

In view of the above consideration, the AP therefore sees reason to set the fine on the basis of the negligent nature of the infringement by € 25,000. But also to pay the fine on the basis of the to reduce the damage-reducing measures taken by € 25,000.

4.3.3 Other circumstances

In its view, Transavia states that those involved with a probability bordering on certainty will not

adversely affected by the data breach. The leaked passenger data did not contain
contact details and were not or only slightly sensitive. Transavia has not had any
reported misuse of the data. Transavia also reported the data breach to the AP in a timely manner
and those involved are informed. Finally, Transavia cooperated as best as possible in the investigation
of the AP and no profits or losses were incurred from the infringement.
The AP is of the opinion that Transavia's cooperation did not go further than its legal obligation
to comply with Article 31 of the GDPR. Transavia has not cooperated with this in a special way
with the AP. Also the circumstance that Transavia only complies with its legal obligation to report to the AP
and data subjects, in view of the seriousness of this violation, the fulfillment of this obligation cannot be regarded as a
alleviating or mitigating factor. Finally, the AP notes that the right of
protection of the personal data of various data subjects has indeed been harmed, because
for example, health data of passengers and contact details of employees are in the hands
came from a malicious third party. These stakeholders are prevented from maintaining the
control of their personal data.
The AP does not give this view in view of the seriousness of the violations and the degree of culpability
reason to waive the imposition of a fine or to cancel 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 to a
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 it can be blamed on Transavia, the damage-limiting measures
and other circumstances taken into account. Due to the large scope 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.

In view of all the circumstances of this case, the AP sees no reason to set the amount of the fine on the basis of

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

in the present case, further increase or decrease.

4.4 Conclusion

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

83 For the motivation, see paragraphs 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. for violation of Article 32(1) and (2) of the GDPR

an administrative fine amounting to:

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

Yours faithfully,

Authority Personal Data,

w.g.

drs. C.E. Mur

board member

Remedies Clause

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

decide to submit a notice of objection digitally or on paper to the Dutch Data Protection Authority. 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 'Making 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'. In your notice of objection, write at least:

- Your name and address
- The date of your notice of objection
- The reference mentioned in this letter (case number); 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).