Authority for Personal Data

PO Box 93374, 2509 AJ The Hague

Hoge Nieuwstraat 8, 2514 EL The Hague

T 070 8888 500 - F 070 8888 501

authoritypersonal data.nl

Social Insurance Bank (Board of Directors)

to the chairman

Mr S.T. Sibma

PO Box 1100

1180 BH AMSTELVEEN

Date

January 19, 2023

Our reference

[CONFIDENTIAL]

Contact

[CONFIDENTIAL]

Subject

Decision to impose a fine

Dear Mr Sibma,

The Dutch Data Protection Authority (hereinafter: AP) has decided to inform the Social Insurance Bank (hereinafter: SVB) to impose an administrative fine of € 150,000 for violation of Article 32, first and second member of the General Data Protection Regulation (hereinafter: GDPR). This is because the SVB is insufficient has taken appropriate measures to ensure a level of security appropriate to the risk with regard to the processing of personal data in the context of telephone customer contact with AOW insured persons.

This decision explains the administrative fine. To this end, (1) the

reason and the course of the proceedings, (2) the established facts, (3) the facts taken by the SVB

improvement measures, (4) the violation and (5) the amount of the fine. Finally (under 6) follows the dictum.

Public version

1

Date

January 19, 2023

Our reference

[CONFIDENTIAL]

1. Reason and course of the process

On November 1, 2109, the AP received a complaint about an alleged infringement related to

personal data at the SVB. The complainant indicated that a family member had personal information about her

would have received from an employee of the SVB, while she had not given the SVB permission

for sharing that information. On the same day, the SVB reported this event as a data breach to the

AP. In that report, the SVB stated, among other things, that unauthorized oral personal data was being used

have been shared with an unauthorized recipient.

By decision of 15 November 2019, the AP informed the complainant that it would not conduct any further investigation

to this event. The complainant appealed against this decision. Following it

the complainant's appeal, the AP has decided to (still) start an investigation. This investigation

focused on compliance by the SVB with Article 5, first paragraph, opening words and under f, in conjunction with

Article 32 of the GDPR for the period from 25 May 2018.

This investigation has led to the AP's Customer Contact and Verifying Investigation Department op

has adopted a report of findings on 4 November 2021 (hereinafter: investigation report). In the

investigation report, it has been concluded that the SVB, pursuant to Article 32, paragraphs 1 and 2, of the AVG

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

to ensure a level of security with regard to the processing of personal data in the framework

of telephone customer contact with AOW insured persons and that the security measures are insufficient

were tailored to the security risks. The Customer Contact and Controlling Investigation Department of the AP has come to the conclusion that from May 25, 2018 until the date of signing the investigation report in violation of article 32, first and second paragraph, of the GDPR, no appropriate technical and organizational measures taken.

In a letter dated 11 November 2021, the AP sent the SVB an intention to enforce.

On 10 December 2021, the SVB submitted a written opinion on this intention and the research report on which it is based, as well as additional information provided to the AP.

An opinion hearing took place on 18 January 2022, during which the SVB presented its written opinion explained orally. After the opinion hearing, the SVB has further details at various times information to the AP.

2. Factual findings in the research report

The following is a summary of the factual findings set out in the investigation report. In his view, the SVB has acknowledged the findings of the investigation report.

1

2

3

4

5

2.1 Organization and tasks involved

6

7

8

9

10

11

The SVB was established pursuant to Article 3(1) of the Work and Implementation Organization Structure Act income (hereinafter: SUWI Act). The SVB is an independent administrative body1 with its own legal personality2.

The SVB is responsible for implementing various related laws and regulations with social security, including the General Old Age Pensions Act (hereinafter: AOW), the General surviving dependents law and the General Child Benefits Act.3 The SVB ensures that customers know to which they are entitled – on the basis of the various laws and regulations – and that they compensation actually received. To fulfill this task, the SVB processes personal data of, among others, insured persons, pensioners, surviving relatives and others benefit claimants.4 The SVB has a total of eleven branches in the Netherlands. Its headquarters based in Amstelveen.

The SVB consists of various directorates and departments. One of these boards is the board of directors 'Social Insurance Services' (hereinafter: DSV). DSV is responsible for, among other things assessing applications for social insurance, including the AOW. Employees of DSV (hereinafter: “service employees”) are also the (telephone) point of contact for customers with questions about social security insurances. Approximately 1500 service employees work for the SVB. The service staff are working spread over ten locations in the Netherlands.

On average, about 20,000 people a week call the SVB with questions about social insurance.

2.2 Operation and content of systems for telephone contact between the SVB and customers.

A service employee uses various systems/applications during telephone customer contact: the [CONFIDENTIAL] system, the Document Management System and the system

[CONFIDENTIAL].

[CONFIDENTIAL] system

The [CONFIDENTIAL] system is the main application for the implementation of the social arrangements at the SVB. The [CONFIDENTIAL] system is divided into a number of subsystems, including client records [CONFIDENTIAL]. The SVB receives data about citizens via the Key Register of Persons (hereinafter: BRP). This data comes from the BRP in [CONFIDENTIAL] justifiably. [CONFIDENTIAL]

1 Article 4, paragraph 1, Suwi Act.

2 Article 3, second paragraph, and Article 4, first paragraph, SUWI Act.

3 Article 34, first paragraph, SUWI Act.

4 Article 35 SUWI Act.

Date

January 19, 2023

Our reference

[CONFIDENTIAL]

12

13

14

15

16

17

Document Management System (hereinafter: “DMS)

All personal documents are included in the DMS, such as all sent and received letters, telephone notes and internal notes (including reports of telephone calls). It's DMS

linked to the [CONFIDENTIAL] system.

[CONFIDENTIAL]

The [CONFIDENTIAL] is the application used by service employees since 2016 to check under look up the files of AOW customers5 during telephone customer contact. [CONFIDENTIAL] is the front-end or user environment of the [CONFIDENTIAL] system.

The figure below shows the [CONFIDENTIAL] screen where service personnel enter the user environment to look up the files of AOW customers. is visible in the blue frame which search combinations service employees can use to look up customers in [CONFIDENTIAL].

[CONFIDENTIAL]

In the following, given the overlap, the distinction between the [CONFIDENTIAL] system and the user environment [CONFIDENTIAL] has been released and the term is used for both systems [CONFIDENTIAL] used.

2.3 Authorizations in [CONFIDENTIAL]

Authorization is the process in which a person is given certain rights within a system.6 The more people have access to data, the greater the risk of data misuse. A system where many individuals having certain access rights to a lot of data therefore entails (many) security risks himself.

The investigation report found that all 1500 service employees of the SVB are authorized to consult all files of [CONFIDENTIAL] AOW customers [CONFIDENTIAL].

5 The legislation and regulations do not refer to customers, but to insured persons, because the AOW is a social insurance. However, the SVB refers to AOW customers. The term 'AOW customers' is therefore also used in this decision.

6 Think of access rights, read rights and mutation rights.

January 19, 2023

Our reference

[CONFIDENTIAL]

2.4 Consulting, sharing and changing (personal) data

18

19

A variety of (personal) data is stored in [CONFIDENTIAL]. It's going down

others, including name and address details, e-mail address, information about nationality, residence permit, living situation,

marital status

state, amount of the benefit, employer details such as payroll tax number, income,

account details, citizen service number and customer studies. It has also been found that if a service employee

has access to the [CONFIDENTIAL] system (and therefore [CONFIDENTIAL]) and the DMS, these also

has access to criminal data in these systems, namely: customer data about a

sentence to detention and its start and end date, data on (suspected) social security

insurance fraud and data on status as a traveler. Since all 1500 service employees

have access to these systems, they therefore have access to all this personal data.

From the foregoing it appears that service employees during telephone contact with AOW customers

can consult the entire file of these customers in [CONFIDENTIAL].

20 The SVB had various work instructions available in an online environment [CONFIDENTIAL].

21

22

23

were for service employees.

The established policy follows from the investigation report and the underlying documents

stipulated that if service employees correctly identify the identity of (an authorized representative of) a

customer, they were allowed to provide and change all customer and legal data7, with

with the exception of information that requires a written form. Furthermore, it turns out

[CONFIDENTIAL] that the BSN is never provided to (authorized representatives of) customers by telephone. Also

stated in [CONFIDENTIAL] that service employees only store address details, bank details and amounts

were allowed to share by phone after asking control questions.

2.5 Authentication

Authentication is the process of verifying a person's supposed identity. A good one

authentication procedure can contribute to an appropriate security policy because it helps unauthorized

prevent access and disclosure of data.

Policy on establishing customer identity on the phone

The investigation report established that the SVB had two work instructions in [CONFIDENTIAL].

which showed how service employees identify the identity of (AOW) customers during the

telephone contact had to be checked.8

7 These are data from customers regarding their entitlement to benefits from national insurance schemes, such as the AOW,

which are administered by the SVB.

8 [CONFIDENTIAL]

The research report concluded that these work instructions differ from each other in terms of content

regarding the method of establishing the identity of the customer on the telephone, and that this

causes confusion among the service staff. The research report also concludes that
many of the prescribed control questions in these work instructions related to relative
easy-to-find information. In one of the work instructions, service employees even became
discouraged from asking for very specific information, such as the date of the last payment or the
net amount of the benefit. In addition, the research report noted that from the
prescribed policy, it was not clear which specific audit questions in any case
must be asked or the minimum number of different control questions that must be asked. In
one of the documents in [CONFIDENTIAL] it was stipulated that in any case to the SVB
registration number [CONFIDENTIAL] or BSN must be requested, while that in the other document
was not prescribed. However, that document did not address the situation in which the caller received this
unwilling or unable to provide information. The policy also offered no clarity on what to do
if there is still doubt about the identity and which (additional) verification questions are subsequently asked
had to be.

Control policy by the SVB

With regard to checking compliance with the authentication policy, the research report
found that the SVB had no adequate way of ensuring that service employees in
checked the identity of customers on the phone in accordance with the policy. That's how it went through
by means of telephone notes drawn up by service employees via a peer test or random sample
verified that customers have been identified in accordance with the policy. In none
however, the telephone notes submitted to the AP contained information about how the
identity of the caller in the telephone conversation was established. Also, there were no fixed formats for it
drafting these notes. During the investigation, the SVB also stated that if the identity
of the caller has been incorrectly established the customer is likely to file a complaint with the SVB and
it is likely that this complaint will be discussed in learning circles set up by the SVB. The SVB also has
stated during the investigation that it was working on a European tender with which the SVB organization
(so also in terms of the implementation of the state pension) would be provided with, among other things, the

automatic recording of telephone conversations in text and the recording of those conversations, in order to optimize phone authentication.

Policy compliance in practice

The research report concludes that, on the one hand, the lack of unambiguous, clear policy and the lack, on the other hand, of an appropriate means of monitoring compliance with this policy has resulted in service staff not (in all cases) following the prescribed instructions in practice followed. Service employees stated differently to employees of the AP about which control questions when they ask during the telephone customer contact. It is also evident from the statements of service employees that they adopt the prescribed (different) working methods

[CONFIDENTIAL] not exactly followed, for example when it comes to the question of how to deal with customers who could not provide the SVB registration number or BSN. The way in which the identity of the calling AOW customers was checked, was therefore apparently to a large extent left to the own judgment and insights of the service employee, is one of the conclusions in the research report.

2.6 Risk-Adapted Policy

Development and evaluation of policy

28

27 When asked by the AP's Customer Contact and Controlling Investigation Department how the policy with with regard to audit questions has been established and to what extent this affects the (security) risk coordinated policy, the SVB has submitted two memorandums from 2006 and 2007, in which this policy is discussed

and of which the SVB considered at that time to be a risk assessment.

The investigation report concludes that in 2006 the SVB identified the risk that a

person requests by telephone to change a payment address, while this person is not the customer. The

SVB then decided to start asking check questions. At a later date, in 2007

an internal SVB memorandum has been drawn up, in which it is emphasized that asking check questions is a less strong

form of authentication is then a construction in which the means of authentication is under the control of the

customer. That note also warns that some care is in order when asking check questions

is; according to that memorandum, the

identity data and also not of data that can be easily retrieved by a third party, such as

name, address, zip code and telephone number. Subsequently, the research report concludes that

the policy had not been changed since 2006 and that there had been no interim evaluations

occurred.

2.7 Awareness

29 Like authentication, awareness is a security measure deployed by the SVB to

30

protect personal data during telephone customer contact. Awareness can make it happen

that employees are more aware of their responsibilities in the field of

information security and act in accordance with their responsibilities.

The research report notes that the SVB employs its employees in different ways

tries to make people aware of the rules and risks of working with personal data, of which the

most awareness methods have a voluntary character. For example, there were work instructions

in [CONFIDENTIAL], although most employees knew who the AP investigators spoke to

not exactly which work instructions about which processes are in [CONFIDENTIAL]. Further are on

the SVB intranet has several pages dedicated to information security. The SVB also has a

code of conduct containing a section on information security, which can be updated by employees

Date

January 19, 2023

Our reference

[CONFIDENTIAL]

entry is signed. Violations of the code of conduct may result in disciplinary action
be affected. Employees who are involved in a data breach are also addressed. Furthermore, in
the investigation report found that the SVB offers some training courses where the rules and risks
of working with (personal) data are treated. The rules are also included in these courses
telephone customer contact. Although these courses were once mandatory for incumbents and
new employees, they were not regularly repeated.

3. Measures taken by the SVB after adoption of the investigation report

In its opinion, the SVB, as noted above, has included the AP's findings in the
research report acknowledged. D SVB emphasizes that privacy protection is of great importance to him. The
In recent years, the SVB has invested heavily in establishing a good privacy organization and -
culture. The SVB considers itself a risk-avoiding organization and in that context is committed to strict security
of its customers' data. In 2021, for example, the SVB will focus on digital resilience and
preventing cybercrime due to constantly evolving cyber risks. The SVB
has mainly focused on preventing attacks involving large-scale personal data
can be extracted.

The SVB recognizes that the investigation report indeed concludes that the protection of
personal data of citizens was not sufficiently guaranteed in the telephone services. In his
view, the SVB has stated in the investigation report that it sees the need and the opportunity to
to significantly improve telephone services to its customers.

31

32

33 Immediately after the AP sent the investigation report to the SVB, on 4 November 2021, the SVB started carrying out a risk inventory and drawing up an action plan. Already on December 9, 2021 – five weeks after the adoption of the investigation report – the SVB issued a extensive risk inventory to the AP, specifically aimed at the telephone service submitted. The risk assessment also specifies which (additional) measures have been taken could be. Incidentally, the SVB has not limited the risk inventory to AOW, but has expanded it to all social security laws falling under the SVB.

Also on December 9, 2021, the SVB submitted a plan of action it has drawn up to the AP provided. This plan contains a package of improvement measures to be implemented in order to meet this come to the findings laid down in the AP investigation report. This package is aimed at, in summary, tightening up the instructions, monitoring compliance with the instructions and improving awareness among its employees.

The SVB then – in accordance with the action plan – already has the following in the first half of 2022 improvement measures actually and concretely implemented.

34

35

* Adjustment/recalibration of the work instructions

On May 31, 2022, the SVB provided revised work instructions to the AP. These work instructions have come to an end became operational in June 2022 and then also placed in [CONFIDENTIAL] and are updated every 2 years evaluated. The following topics, among others, are included in the work instruction:

- with which control questions the service employee should start;

- which additional verification questions the service employee should ask. The service person must assess, given the specific situation, which audit questions are appropriate (tailor-made), but the work instruction has no non-binding character. For example, it is prescribed which questions the service employee must ask in any case and how many control questions he must ask (minimum).

- when the service employee has reason to doubt the identity of the caller;

- what the service employee should do if the doubt is not resolved;

- that the service employee must record in what way the identity has been checked and which audit questions are asked;

- which personal data may not be provided by the service employee by telephone.9

In addition, the SVB has decided to implement the work instructions for the entire site under its jurisdiction recalibrate social security laws, so not only for the state pension (AP research scope).

The work instructions will also be evaluated periodically (every two years).

* Structured recording of audit questions (system support)

As noted in section 2.5, the SVB has already stated during the ongoing AP investigation that it is working with a European tender with which the entire SVB (and therefore also with regard to the implementation of the AOW) would be equipped with, among other things, the automatic recording of telephone conversations in text and recording those conversations, in order to optimize telephone authentication. It is the intention that listening back to the control questions asked by service employees is a take on an ongoing character and that they are analysed; the so-called feedback loop.

In May 2022, the SVB, to promote awareness and to monitor compliance with the work instruction possible, an entry field in the (AP assumes: [CONFIDENTIAL]) system incorporated. In this, service employees – as input for their telephone note – must enter the complete verification questions to determine the identity of the caller.

* Periodic deployment of mystery callers (awareness, testing and assurance)

From the second quarter of 2022, the SVB will use so-called mystery callers. This mystery

callers call a service employee on behalf of the SVB and provide feedback to the SVB on which how the service employee has checked the identity. The SVB evaluates the conversation with the

9 This includes BSN, criminal data and special personal data (health, nationality, ethnicity).

service employee and shares the learning points (in a general sense) with other employees. This is a fixed become part of the learning curve of the service employees.

* Ongoing campaign (awareness)

To raise awareness, the SVB has drawn attention to the AP's findings of its service personnel. In addition, the SVB has included in its action plan continuously pay attention to privacy protection during telephone customer contact, for example via the SVB intranet, in internal newsletters and organisation-wide meetings.

* Customization of the phone training (craftsmanship)

From the first quarter of 2022, the SVB has adjusted its existing telephone training. The awareness is increased in terms of caller identification, authentication and sharing of information by telephone. This adjustment is reflected in all telephony training courses and will be phased offered to both new and experienced service personnel. The SVB monitors the (mandatory) participation and compliance with the training courses and also organizes - to prevent knowledge blurring - refresher courses.

4. Assessment

4.1 Scope GDPR

36

37

Pursuant to Article 2, paragraph 1, of the GDPR, this Regulation applies to the whole or in part automated processing, as well as to the processing of personal data contained in a file included or intended to be included therein.

Pursuant to Article 3, paragraph 1, of the GDPR, this regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, whether or not the processing takes place in the Union does not take place.

4.2 Processing of (criminal) personal data and responsibility for processing

4.2.1 Legal framework

38 Pursuant to Article 4, preamble and under 1, of the GDPR, personal data is understood to mean all information about an identified or identifiable natural person (the data subject). Like a identifiable natural person must be considered a natural person who is directly or indirectly can be identified.

39 Under the GDPR, more safeguards apply to the processing of criminal data, because these data relate to behaviors that give rise to social disapproval, so that

the fact that access is granted to such data may stigmatize the data subject and thus could seriously infringe his private or professional life.10 Article 10 of the GDPR describes criminal data such as personal data concerning criminal convictions and criminal offenses

facts or related security measures.

Article 4, preamble and under 2, of the GDPR stipulates that the processing of personal data is

means an operation or a set of operations with regard to personal data or a set

of personal data, whether or not carried out through automated processes, such as collection,

recording, organizing, structuring, storing, updating or changing, retrieving, consulting, using,

provide by transmission, distribution or otherwise making available,

align or combine, block, delete or destroy data.

Recital 15 of the GDPR states that to avoid a serious risk of circumvention

arise, the protection of natural persons should be technology neutral and not dependent

may be of the technologies used. The protection of natural persons should apply to

both automated processing of personal data and manual processing thereof if the

personal data are stored or are intended to be stored in a file.

Article 4, preamble and under 7, of the GDPR stipulates that controller is understood

a natural or legal person who, alone or jointly with others, has the purpose of and the means

for the processing of personal data; when the objectives of and the means for

whether such processing is established in Union or Member State law may be determined therein

who the controller is or according to which criteria they are designated.

Article 35, first paragraph, of the SUWI Act stipulates that the SVB is the controller for the

processing of data about insured persons and beneficiaries within the meaning of the national insurance schemes

and about persons belonging to the insured in the insured administration.

4.2.2 Assessment

Personal data

In paragraphs 2.2 and 2.4 of this decision it is explained that the SVB in [CONFIDENTIAL] of

[CONFIDENTIAL] AOW customers, has stored various categories of personal data, such as

Name and address details, employer details, BSN, date of birth or marital status. Also are in

[CONFIDENTIAL] and DMS where applicable customer data stored on a

sentence to detention and about the start and end date thereof, information about (a suspicion of)

social insurance fraud and data on status as a traveller.

40

41

42

43

44

45

The data related to detention qualify as criminal data

convictions, as detention is the result of a criminal conviction or a well-founded one

10 CJEU 22 June 2021, C-439/19, ECLI:EU:C:2021:504 (Latvijas Republikas Saeima (Point de pénalité)), r.o. 75.

suspicion of a criminal offense. Data on travelers and social security fraud can

also qualify as data relating to criminal offenses as it concerns data about

well-founded suspicions of criminal offenses or social insurance fraud11 and participation

to a terrorist organization12.

46 Based on the above, the AP concludes that in [CONFIDENTIAL] and DMS both regular

personal data is stored as personal data concerning criminal convictions and

criminal offenses within the meaning of Article 4, preamble and under 1, of the GDPR and Article 10 of the GDPR.

Processing

47 For this, the AP has concluded that the SVB has different categories in [CONFIDENTIAL] and DMS

has stored personal data of AOW customers. The personal data entered in [CONFIDENTIAL]
are stored, are frequently used, consulted, updated, changed or made available by the SVB
made available in the context of the telephone contact that service employees have with AOW pensioners
customers and third parties. The AP therefore concludes that personal data is processed in the
meaning of Article 4, preamble and under 2, of the GDPR.

48

49

50

Controller

As follows from marginal number 43 of this decree, the SVB is responsible for the processing
of personal data in the implementation of national insurance schemes. The AOW is one of those
national insurance schemes, so that the AP concludes that the SVB qualifies as a controller
for the processing of personal data in the context of the AOW.

4.3 Security Obligation

4.3.1 Legal framework

Article 32, paragraph 1, of the GDPR reads, insofar as relevant here: “Taking into account the state of the
technique, implementation costs, as well as the nature, scope, context and processing purposes
and the varying likelihood and severity of risks to the rights and freedoms of individuals,
the controller and the processor shall take appropriate technical and organizational measures
measures to ensure a level of security appropriate to the risk (…).”

Article 32, second paragraph, of the GDPR reads: “When assessing the appropriate security level
in particular taking into account the risks of processing, in particular resulting from the destruction, loss,
the modification or the unauthorized provision of or unauthorized access to forwarded, stored
or otherwise processed, whether accidentally or unlawfully.”

11 See Article 84 of the SUWI Act.

12 See, among others, Article 140a of the Criminal Code.

51

52

53

54

The risk to the

rights and freedoms of persons. Recital 15 of the GDPR states that in terms of probability

and seriousness ultimate risk to the rights and freedoms of natural persons may arise from

personal data processing that can result in serious physical, material or immaterial damage,

in particular:

“- where the processing may lead to discrimination, identity theft or fraud, financial loss,

reputational damage, loss of confidentiality of data protected by professional secrecy,

unauthorized reversal of pseudonymization, or any other significant economic or

social disadvantage;

- when the data subject cannot exercise their rights and freedoms or are prevented from monitoring

over their personal data;

- (…) in the processing of (…) criminal convictions and offenses or related thereto

containing security measures;

- (…);

- when the processing involves a large amount of personal data and has consequences for a large

number of people involved.”

With regard to determining appropriate measures, recital 83 of the GDPR states that those measures should provide an appropriate level of security, including confidentiality guarantees, taking into account the state of the art and the implementation costs compared to the risks and the nature of the personal data to be protected. When assessing the data security risks, attention should be paid to risks that arise at personal data processing, such as destruction, loss, alteration, unauthorized provision of or unauthorized access to the transmitted, stored or otherwise processed data, whether accidental or unlawful, which in particular involves physical, material or can lead to immaterial damage.

Section 41(1) of the Autonomous Administrative Bodies Framework Act stipulates that an independent administrative body, on the basis of the relevant regulations applicable to the Central Government, ensures the necessary technical and organizational facilities to protect his data against loss or damage and against unauthorized access, alteration and provision of data.

Regulations for the necessary technical and organizational facilities for the security of data within the government are laid down in the Baseline Information Security Government (hereinafter: BIO). The The AP's Customer Contact and Controlling Investigation Department has the following provisions from the BIO involved in her research:

- Objective: To ensure that employees and contractors are aware of their information security responsibilities and fulfill them (BIO standard 7.2);
- Management should require all employees and contractors to practice information security apply in accordance with the established policies and procedures of the organization

[CONFIDENTIAL]

(BIO standard 7.2.1); and

- All employees of the organization and, where relevant, contractors are given an appropriate

awareness education and training, and regular refresher courses on policies and procedures

of the organization, insofar as relevant for their position (BIO standard 7.2.2).

4.3.2 Risk assessment assessment

55 In the opinion of the AP, at the time of signing the investigation report, the SVB,

November 4, 2011, does not have an adequate risk assessment. Insofar as there was any risk

inventory, it was dated and incomplete.

56

57

During the AP's investigation, the SVB provided two memorandums from 2006 and 2007 to the AP on request.

submitted, in which this policy is discussed and which the SVB considered to be a risk assessment

is made.13

However, these two notes cannot be regarded as a (proper) risk inventory. This

notes were 14 years old at the time of signing the research report and therefore very

dated. The AP also notes that - apparently - there has been no interim reassessment of the risks

occurred.

58 In the opinion of the DPA, these two memorandums cannot be classified as risk

inventory in which the specific risks are identified and assessed on the basis of the

probability of its occurrence and the seriousness of the adverse consequences for the person concerned

persons. Both memorandums address the risk of someone calling the SVB wrongly

pretends to be a customer, but does not address (the seriousness of) the adverse consequences for the customer

or on the likelihood of this risk occurring. Moreover, not all risks are listed in the notes

named. For example, no attention is paid to the fact that all 1500 service employees have access

to all personal data of [CONFIDENTIAL] AOW customers, including BSN, financial and

criminal data, and the risks associated with such large-scale access.

4.3.3 Risk assessment

59 The AP is of the opinion that the risks to the rights and freedoms of natural persons are associated with deal with the telephone service, partly in view of the scope of the processing, the nature of the processed data, the large number of authorized employees and the frequency with which customers contacting the SVB by telephone, should be regarded as high.

60

It has been established that a very large group of stakeholders, namely [CONFIDENTIAL] AOW customers, personal data is stored in the systems of the SVB. It has been established that the SVB has a wide range of personal data of these AOW customers, such as name and address details, telephone number,

13 See section 2.6 of this decision.

date of birth, country of birth, citizen service number, bank account number, information about a possible partner, amount of the benefit and employer data. In addition, the SVB also disposes of this in some cases on personal data relating to criminal convictions and offences. These are very sensitive data that must be particularly protected. The consequences of (unlawful) disclosure of such data can be very far-reaching.14

61

In addition, it has been established that all 1500 service employees have the data of [CONFIDENTIAL] AOW-customers can view. Such an 'open' authorization system undeniably poses security risks with them. The more people have access to this system, the greater the risk of data misuse.

62 It has also been established that the SVB pursues a policy whereby (AOW) customers can, among other things, receive information
request and pass on changes and that there are an average of 20,000 people with the SVB every week
calling.15 Without appropriate security measures, this can lead to unauthorized use of the telephone
personal data is provided or changed.

63 The chance that third parties try to gain access on a large scale by telephone via service employees of the SVB
however, the AP does not consider it likely. However, there is a chance that third parties will contact the
SVB to obtain information about someone they know that they do not represent. In the
The complaint referred to in marginal number 1 of this decision has also prompted the AP to conduct an investigation
start.

64 In view of the foregoing, the AP assesses the risks of these data processing for the individual
AOW customer as high. For example, personal data can be shared or changed with or by a
unauthorized, which in certain cases can have serious consequences for the data subject. In individual
cases, serious material and immaterial damage is conceivable. This may include the risk
of damage due to unauthorized use of data. [CONFIDENTIAL]. This can have major consequences
for the person concerned, not just financial. In addition, there is a real risk that acquaintances of state pension
customers try to retrieve or change information from the SVB for personal reasons, what would
can lead to, for example, stalking or extortion. Finally, there is the risk of damage to reputation
sharing of personal data related to criminal convictions and offences.

4.3.4 Assessment of appropriate security measures at the time of signing the investigation report

65 The AP is of the opinion that – in view of the risks described above – the measures taken by SVB at the time of
the determination of the research report had taken in terms of authentication and awareness
were insufficient or that those measures insufficiently mitigated the security risks to lead to a
level of security appropriate to those risks. The AP explains this.

14 See paragraph 2.4 of this decision.

15 See sections 2.1 and 2.4 of this decision.

Phone Authentication Policy

66 It is true that the SVB had drawn up a policy regarding checking the identity of callers
through (control) questions, but the AP has determined that this policy is divided into two separate
work instructions were available [CONFIDENTIAL], each of which has a different working method
description.16 The policy was therefore not unequivocal, which meant that it was also not for the service employees
it was clear which of the two instructions was correct and had to be followed.

67 In addition, more than half of the audit questions related to information that was easy to retrieve.
For example, it followed from the internal SVB policy that it was possible to ask for a combination of address and
date of birth of the data subject, which offers a low level of security protection because
Name and address details are available for a large number of people. For example, this data is often
known to friends, family and (former) colleagues. In addition, this information is easy to access
from public sources, including social media.

68

Furthermore, only one of the [CONFIDENTIAL] pages required service personnel to
ask for either the SVB registration number [CONFIDENTIAL] or the BSN. For these numbers
applies that the protection level is higher than with name and address data, because these identification numbers are in
will generally only be accessible to a select circle around the data subject.
However, in this instruction, service employees were left free to choose which additional
control questions, when they should be asked. This work instruction also did not indicate whether there were any data
may be provided or changed if the customer has his or her SVB registration number [CONFIDENTIAL]

or BSN, so it was unclear to service employees what to do in that case

do.17

69 Admittedly, it followed from the policy that if the service employees still had doubts after the first questions

the identity of the caller, the employees had to ask additional verification questions. Policy

however, did not clarify in which situations doubts should still arise about the

identity and which (additional) verification questions had to be asked in that case.18

70

71

Finally, it was found that the service employees do not follow the available policy carefully and in detail

consistently complied.19 Service employees had, experienced or accepted in the performance of their

apparently a certain degree of freedom.

Checking the phone authentication policy

At the time of signing the investigation report, the SVB also had no adequate way to

Verify that service personnel identify customers in accordance with policy

16 See section 2.5 of this decision.

17 Ibid.

18 Ibid.

19 Ibid.

checked the phone. As noted above, although by means of

telephone notes drawn up by service employees via a peer test or random check whether the

Customer identities were established in accordance with the policy, but were not in any of the cases
the AP submitted phone notes included information on how the caller's identity was in it
phone call was established. There were also no fixed formats for drawing up these notes.20
As a result, there was no incentive for service employees to make them work in their
telephone notes recorded how they established the identity of the caller. It is true that the SVB has during
the AP investigation stated that it is working on a European tender with which the entire SVB (and therefore
also AOW) would be provided with, among other things, the automatic recording of telephone conversations
text and call recording which would become the practice around phone authentication
improved, but this tender process had not yet been completed, so at the time of signing
of the research report, the aforementioned omissions still existed.
As stated in marginal number 25 of this decision, the SVB also has during the investigation
stated that if the caller's identity has been incorrectly established, the customer is likely to receive a
will submit a complaint to the SVB and it is likely that this complaint will be discussed by the SVB
organized learning circles.21 If a means of control is based on such an assumption, then that is the
opinion of the AP by definition inadequate. After all, only a check takes place in that case
a customer is aware that another person has unauthorized information about him or her
obtained and that customer also actually submits a complaint to the SVB.
Awareness
Controllers must ensure that their employees are aware of their
information security responsibilities and act in compliance with them
responsibilities.
The SVB uses various awareness-raising methods. In this case, the AP considers in particular the
work instructions in [CONFIDENTIAL] and the training courses offered by the SVB are relevant, since
it specifically mentions how service employees should handle the processing of
personal data in the context of telephone contact with customers.

73

74

75 In the opinion of the AP, at the time of the adoption of the investigation report, the organizational measures that the SVB had taken in the field of awareness to protect personal data insufficient.

76 It is true that the SVB had one-off mandatory training courses that covered the rules and risks of working with (personal) data during telephone customer contact were treated, but the frequency of the training was low. In addition, the work instructions [CONFIDENTIAL] are available at all times

20 Ibid.

21 Ibid.

were, but that it was up to the employees to consult these work instructions (periodically). The result of this was that the employees were not always aware of the (most) recent instructions. It also turned out that the working method of service employees deviated from the standard with some regularity method prescribed in the different awareness methods. A regular further training of the rules and procedures related to the security of personal data in the framework of telephone customer contact was lacking, with the risk that more experienced employees were gradually able to deviate from the policy – which actually happened in practice.

4.3.5 Conclusion on security measures

77

The AP reiterates its conclusion that at the time of the adoption of the investigation report, the SVB (still)

had not carried out an adequate risk assessment. Insofar as there was any risk
inventory, it was dated and incomplete. In addition, in the opinion of the AP, the risks must be quantified
associated with the telephone service, partly in view of the scope of the processing
([CONFIDENTIAL] AOW customers), the nature of the processed data (including financial and
criminal records), the large number of authorized employees (all 1500 service employees)
and the frequency with which people contact the SVB by telephone (an average of 20,000 times per year).
week22), are considered high. In view of this high risk, in the AP's opinion the
measures taken by the SVB in terms of caller authentication and awareness
inadequate.

78 With regard to the assessment of whether the security measures are appropriate, account should be taken, among other things
into account the implementation costs of those measures. In the opinion of the AP there are none
large implementation costs involved in (substantially) improving the security measures. That
applies, for example, to drawing up a good, unambiguous working method with regard to the
verify the identity of the caller. Also increasing the compliance rate of the
security policy for telephone customer contact, no disproportionate implementation costs are involved.

79

80

In view of the foregoing, the AP concludes that SVB's security measures are not appropriate
were in relation to the security risks in the processing of personal data by telephone
customer contact with AOW customers. The AP concludes from this that the SVB has acted in violation of
Article 32, first and second paragraph, of the AVG.

4.4 Duration of the Violation

The investigation report signed on November 4, 2021 concluded that from May 25, the SVB
2018 had not taken appropriate technical and organizational measures to mitigate the risk
ensure a tailored level of security with regard to telephone customer contact with AOW pensioners

22 This concerns the total number of questions per week regarding all social security laws. The AP does not know which one percentage of this relates to AOW, but since, according to the SVB, approximately 63% of the population is entitled to AOW, it can be

assumed that a substantial part of the telephone questions pertain to the AOW.

81

82

83

customers. The SVB recognizes this. As explained above in Chapter 3 of this decision, the SVB has as soon as the research report of the AP became known immediately and energetically worked on the improvement of the security of the processing of personal data during telephone customer contact.

As of December 9, 2021, the SVB has an extensive service specifically aimed at telephone services risk inventory submitted to the AP. This risk inventory is not limited to the AOW, but is aimed at all social security laws falling under the SVB. In the opinion of the AP are in this inventory the (specific) risks associated with the processing of personal data in the context of telephone customer contact is sufficiently identified and assessed on the basis of the likelihood of those risks occurring.

In December 2021, the SVB also adopted an action plan in which a package of improvement measures has been included to mitigate the risks associated with its telephone services to limit. Immediately after the adoption of this action plan, the SVB started with the its implementation, which resulted in a large number of

improvement measures have actually and concretely been implemented in the field of recording,
system support, testing and assurance, craftsmanship and awareness.
For example, the SVB has adjusted its policy with regard to telephone authentication by the two old ones
replace work instructions with one new, unambiguous, clear and for the service employees
centrally accessible work instructions that prescribe the procedure for telephone authentication of
callers. The way in which the identity of the calling AOW customers is checked is in
left to a considerably lesser extent to the service representative's own judgment and insights.
The work instruction clarifies which control questions a service employee should start with, which ones
additional control questions a service representative should ask, which questions a service representative should ask
must ask in any case, how many control questions a service employee must ask (minimum),
when a service employee has reason to doubt the identity of the caller and what a
service representative should do if the doubt is not cleared. It's also clearer
service employees should do if customers cannot or cannot find the [CONFIDENTIAL] number or social security number
want to provide. Service employees are therefore less free to choose which (additional)
they ask when they can ask and what they should do if there is still doubt about the identity
from the caller. Furthermore, the DPA has established that the audit questions do not only relate to easy to
retrieve data. These instructions therefore also contribute to an increased level of awareness
of the service employees. In addition, a periodic (biennial) evaluation by the SVB makes a
fixed part of the process, which makes a positive contribution to the security level of the
telephone service.
84 From now on, service employees will also enter information in their telephone notes – via an entry field
[CONFIDENTIAL] – structured record of which control questions they have during a telephone conversation
provided to verify the identity of the caller. In this way, the SVB can gain awareness

expand its organization. In addition, this allows the SVB to check how the identity is verified of callers in practice, form an opinion on this and possibly take further improvement measures meet. The introduction of a periodic deployment of mystery callers, whereby the SVB also pays the mystery caller evaluates the conversation with the service employee and the learning points in a general sense shares with other employees, further promotes both control and awareness level.

85 In addition, the SVB has included an ongoing awareness campaign in its action plan in which attention is regularly paid to privacy protection during telephone customer contact, for example via the SVB intranet, in internal newsletters and organisation-wide meetings.

86 In addition, it is relevant that the SVB is updating its existing (compulsory for service employees) telephone training has adapted to raise awareness in terms of caller authentication and sharing information by telephone even further. This adaptation is offered to both new as experienced service employees. The SVB also organizes refresher courses.

87 In the AP's opinion, the SVB has already taken advantage of the introduction of these improvement measures June 2022, appropriate and organizational measures have been taken that are tailored to the risk ensure security level.

4.5 Conclusion

88 In view of the foregoing, the AP is of the opinion that, although the SVB has introduced improvement measures, the SVB has nevertheless violated article 32, first and second paragraph, of the AVG. That offense consists that the SVB has failed to take appropriate technical and organizational measures at a risk ensure an appropriate level of security with regard to the processing of personal data the context of telephone customer contact with AOW customers. This violation lasted from May 25 2018 to June 2022.

5. Fine

89

5.1 Introduction

Any processing of personal data must be done properly and lawfully. To avoid that

organizations with the processing of personal data infringe on the privacy of citizens

It is very important that they apply a security level appropriate to the risk.

90 The SVB has acted contrary to article 32, paragraphs 1 and 2, of the GDPR. As a result, the SVB

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

as referred to in Article 5 GDPR. The AP therefore uses its authority to submit a

to impose a fine. Because the SVB has meanwhile energetically reversed this violation and there

in view of the improvement measures taken by the SVB, there is no fear that these will be repeated

violation, the imposition of an order subject to periodic penalty payments is no longer an issue.

5.2 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 and seventh paragraph,

of the GDPR,

read in conjunction with Article 18(1) and (2) of the General Ordinance Implementation Act

data protection (hereinafter: UAVG), the AP is authorized to report to the SVB in the event of a violation of

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

91

92

The AP has established fining policy rules23 (hereinafter: de

Fining policies). The system of the Fining Policy Rules is as follows.

93 The violations for which the AP can impose a fine up to the amount stated above are listed in the Fining policy rules divided into three fine categories. These categories are ranked by weight of the violation of the said articles, where category I contains the least serious violations and category III the most serious offences. The categories are subject to increasing fines connected. This follows from Article 2, under 2.1 and 2.3 of the Fining Policy Rules.

Category I

Category II

Category III

Fine bandwidth between € 0 and € 200,000

Fine bandwidth between € 120,000 and € 500,000

Fine bandwidth between € 300,000 and € 750,000

Basic fine: €100,000

Basic fine: €310,000

Basic fine: €525,000

94 Violation of Article 32 of the GDPR (security of processing) is, according to Annex I to the Fining policy rules, classified in category II. As follows from the table above, applies to this category a fine range between a minimum of €120,000 and a maximum of €500,000, with a basic fine of €310,000.

95 The basic fine applies as a neutral starting point and should be increased or decreased insofar as the factors stated in Article 7 of the Fining Policy Rules give rise to this. The final height of the fine must be proportionate and geared to the seriousness of the violation and the extent to which it occurs can be blamed on the offender.24

23 Fining policy rules of the Dutch Data Protection Authority of 19 February 2019 with regard to determining the amount of administrative fines (Fine Policy Rules of the Dutch Data Protection Authority 2019), Stcrt. 2019, 14586, March 14, 2019.

24 Compare Article 49, paragraph 3 of the Charter of Fundamental Rights of the European Union (hereinafter: the Charter)

and Articles 3:4

and 5:46 of the General Administrative Law Act.

5.3 Fine amount

96 In the AP's opinion, a number of mitigating circumstances and proportionality lead to

significant reduction of the (basic) fine. The degree of culpability of the conduct does not matter

cause for further adjustment of the fine.

5.3.1 Mitigating Circumstances

97 The factors stated in Article 7, preamble and under a and c of the Fining Policy Rules give rise to the

98

to reduce the basic fine.

It has been established that the SVB processes various categories of personal data of very many data subjects.25

As explained in section 4.3.3 of this decision, this can have major consequences for those involved.

Although there is a chance that third parties will contact the SVB by telephone with the aim of obtaining information

obtaining information about someone they know and whom they do not represent can be countered in this case

be stated that those third parties in that contact come into direct contact with a service representative,

which raises a certain threshold. In addition, the SVB had already taken measures in its policy

with regard to the provision of information during telephone customer contact, which the AP considers limiting the risk

considers. For example, in the event that service employees correctly identified (a

authorized representative of) a customer, do not provide and change data for which a

written form is required. Service employees were also allowed to provide address details, bank details and amounts

only provide by telephone after asking (additional) verification questions. The BSN were allowed
never provide service employees to (authorised representatives of) customers. Thus existed telephone
access to a more limited amount of personal data. Also with the introduction of the new telephone
authentication policy, the SVB has drawn up a list in which it is made explicit that the following data
may not be provided by telephone: the BSN, criminal data (such as data about – the
evade – detention) and special personal data, such as data about the health of
a person, nationality and ethnicity (e.g. country of birth, country of origin).

99 Although cases of unauthorized access via telephone customer contact are not always (directly) by the SVB
will be noticed, it is very likely that the number is due to the old telephone
authentication policy affected data subjects is low. Unlike is often the case with, for example, a
burglary in a computer system of a controller, is in case of telephone customer contact
no unauthorized access to entire customer files. Third parties can only
always obtain information from a specific data subject in individual cases by conducting
skillful conversations with a service representative.

25 The SVB has stored various categories of personal data in [CONFIDENTIAL] of [CONFIDENTIAL] AOW customers,
such as name and address details, employer details, BSN, criminal details, date of birth or marital status.

100 Information provided by the SVB also shows that an average of about 20,000 people per week go to the
Call the SVB with questions about social insurance. This, while the SVB in the period 2018 to 2021
has only detected ten data breaches in relation to the provision of data to an unauthorized person
person via telephone service. Moreover, only three of those data breaches related to

AOW customers and only saw one data breach – the data breach that gave rise to the present one
investigation by the AP – on telephone authentication. The SVB also has an agreement with that person
agreed on compensation.26

101 In view of the foregoing, the DPA sees, pursuant to Article 7, preamble and under a and c, of the
Fining policy rules give rise to a reduction in the base amount of the fine.

5.3.2. Blameability and proportionality

102 Pursuant to Article 5:46, second paragraph, of the General Administrative Law Act (hereinafter: Awb), the AP keeps
the imposition of an administrative fine takes into account the extent to which it can be imposed on the offender
blamed. Article 32 of the GDPR does not contain intent or guilt as an element. As follows, inter alia, from the
judgment of the Administrative Jurisdiction Division of the Council of State of 27 March 2013,
ECLI:NL:RVS:2013:BZ7467, may then in principle be regarded as the culpability of the violation
gone out. If a controller argues that he has no
only reproach can be made, he will have to make this plausible.27

103 The SVB is obliged to provide an op
risk-appropriate level of security. The SVB can be blamed for not complying with this
obligation has been fulfilled. The AVG, but also the BIO with which the SVB must comply, has with regard to
the security of the processing of personal data explicitly described that organizations have an op
risk-appropriate level of security. The SVB can be expected to
of the standards applicable to him and acts accordingly. Now that the violation the SVB can fully
be blamed, the degree of culpability of the offense does not give rise to it
to reduce the fine.

104 Finally, pursuant to Article 49, paragraph 3 of the Charter and Articles 3:4 and 5:46 of
the Awb or the application of its policy for determining the amount of the fines in view of the
circumstances of the particular case, does not lead to a disproportionate outcome.

26 Report of the opinion hearing of 18 January 2022, p. 10.

27 Compare the judgments of the Administrative Jurisdiction Division of the Council of State of 29 August 2018

(ECLI:NL:RVS:2018:2879,

oh. 3.2) and 5 December 2018 (ECLI:NL:RVS:2018:3969, issue 5.1). Also compare the decisions of the Appeals Board for it industry of 29 October 2014 (ECLI:NL:CBB:2014:395, ow. 3.5.4), 2 September 2015 (ECLI:NL:CBB:2015:312, ow. 3.7) and 7 March 2016 (ECLI:NL:CBB:2016:54, issue 8.3). Finally, see Parliamentary Papers II 2003/04, 29 702, no. 3, p. 134.

105 In view of the proportionality of the fine to be imposed, the AP considers it important that the SVB is very proactively started working with the findings from the AP research report. Already five weeks after the signing and sending the investigation report, the SVB provided the AP with an extensive risk assessment inventory and an action plan. Subsequently, the SVB acted entirely of its own accord very quickly a large number of improvement measures actually and concretely implemented in the field of recording, system support, testing and assurance, craftsmanship and awareness. All these actions led to the SVB committing the violation within six months of signing the investigation report has ended, without an enforcement decision by the AP as the basis for this lay. In addition, it is also taken into account that the SVB will already be independent (without the intervention of the AP) in December 2021.

has decided to use the revised work instructions not only for the AOW, but for the entire site of social insurances falling under him. All measures taken and the In any case, the speed of this shows the willingness of the SVB to take security seriously in the organization to get started.

106 In view of the foregoing, the AP sees reason to set the amount of the fine on the basis of proportionality further reduced to an amount of € 150,000.

5.4 Conclusion

107 The AP sets the fine amount for the violation of Article 32, paragraphs 1 and 2, of the GDPR, in view of the foregoing fixed at € 150,000.

6. Operative part

The AP submits to the Social Insurance Bank for violation of Article 32, first and second paragraph, of the GDPR, an administrative fine amounting to: € 150,000 (in words: one hundred and fifty thousand euros).28

Yours faithfully,

Authority for Personal Data,

e.g.

Mr. A. Wolfsen

chair

Remedies Clause

If you do not agree with this decision, you can within six weeks from the date of sending it decides to submit a notice of objection digitally or on paper to the Dutch Data Protection Authority. In accordance Article 38 of the UAVG suspends the effect of the decision until submitting a notice of objection imposition of an administrative fine. The AP will only proceed with collection after the decision has become irrevocable.29 For submitting a digital objection, see www.autoriteitpersoonsgegevens.nl, under the heading Objecting to a decision, at the bottom of the page under the heading Contact with the Dutch Data Protection Authority. The address for submission on paper is: Dutch Data Protection Authority, PO Box 93374, 2509 AJ The Hague.

Mention 'Awb objection' on the envelope and put 'bezwaarschrift' in the title of your letter.

Write in your notice of objection at least:

- your name and address;

- the date of your objection;

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

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

- your signature.

28 The AP will hand over the aforementioned claim to the Central Judicial Collection Agency (CJIB). The fine should be accordingly

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

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

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