Authority for Personal Data

PO Box 93374, 2509 AJ The Hague

Bezuidenhoutseweg 30, 2594 AV The Hague

T 070 8888 500 - F 070 8888 501

authoritypersonal data.nl

Registered

UWV

Board of Directors

PO Box 58285

1040 HG Amsterdam

Date

July 31, 2018

Subject

Load under duress

Resume

Our reference

z2018-02009

Contact

[CONFIDENTIAL]

070 8888 500

1.

2.

3.

4.

5.

On March 27, 2017, the Dutch Data Protection Authority (hereinafter: the AP) has, on the basis of Article 60 of the

Personal Data Protection Act (hereinafter: the Wbp), as it applied at the time, initiated an investigation to the use of multi-factor authentication in the employer portal of the Implementation Institute Employer insurance (hereinafter: the UWV).

In the employer portal, the UWV processes, among other things, personal data relating to the employee health. In view of this, access to the employer portal must take place via the internet found through multi-factor authentication. The UWV currently applies one-factor authentication to the providing access to the employer portal.

In the final findings report (hereinafter: the investigation report), the AP has established that the UWV thus acts in violation of Article 13 of the Wbp, as it applied at the time, on the basis of which, for insofar as relevant here, a controller must take appropriate measures to process personal data secure against loss or against any form of unlawful processing.

The AP bases the penalty decision on the investigation report, which was given orally by the UWV view on the intention of the AP to impose an order subject to periodic penalty payments and the subsequent decision by the UWV provided information at the request of the AP

On May 25, 2018, the General Data Protection Regulation (hereinafter: the GDPR) applies become. In Article 32, first paragraph, the GDPR imposes the same obligation as it applied under Article 13

Annex(es) 2

1

Date

July 31, 2018

Our reference

z2018-02009

6.

7.

8.

9.

10.

11.

12.

13.

of the Wbp. Now that this violation still continues, the UWV violates article 32, first paragraph, of the
AVG.

The UWV wishes to connect to the eHerkenning system in order to enable multi-factor authentication.
when granting access to the employer portal. The date on which UWV
expects that it will only be possible to log in to the employer portal by using eHerkenning
since the first request by the AP by letter of 25 November 2015 has now been moved to
November 1, 2019.

In response to the above, the AP has decided, pursuant to Article 16, paragraph 1, of the
General Data Protection Regulation Implementation Act (hereinafter: UAVG) viewed in conjunction with
Section 5:32, subsection 1, of the General Administrative Law Act (hereinafter: the Awb) imposes an order subject to periodic
penalty payments
to lay. With the order subject to periodic penalty payments, the AP aims to ensure that the established violation is met
an end is made.

By 31 October 2019 at the latest, granting access to the employer portal of an appropriate
security level are provided, whereby logging in to the portal is only possible by means of a
appropriate form of multi-factor authentication. Part of that burden is that the UWV required it
confidence level should be re-determined by performing a risk analysis based on the
most recent version of the Handbook 'Reliability levels for digital services, an
guide for government organizations' (version 4).

If the order is not complied with after the grace period has expired, the UWV will be subject to a penalty of
EUR 150,000 due for each month that the order is not (fully) executed, with a maximum
of EUR 900,000.

Course of the procedure

On August 29, 2017, the AP adopted the investigation report and sent it to the UWV.

The public version of the report was published on November 14, 2017 on the AP website.

In a letter dated 15 August 2017, the AP has sent a few more questions to the UWV as a result of the investigation questions about the size of the employer portal.

In a letter dated 30 August 2017, the UWV responded to the questions posed by the AP in a letter dated 15 August 2017 has stated.

In a letter dated 11 September 2017, the UWV responded to the investigation report. The UWV indicates that it recognizes, among other things, that the security level does not meet the requirements of Article 13 of the Wbp and want to remedy this by implementing eHerkenning level substantial.

Date

July 31, 2018

Our reference

z2018-02009

14.

15.

16.

17.

18.

19.

In a letter dated 9 November 2017, the UWV informed the AP about the progress of the implementation of eHerkenning.

The AP informed the UWV by letter dated 14 December 2017 of its intention to subject to periodic penalty payments and the UWV has been given the opportunity to do so orally or in writing

to put forward a point of view. The UWV has been invited for a hearing.

The hearing took place on 6 February 2018. A record has been made of the hearing

annex 1 is attached to this decision.

In response to what was discussed during the hearing, the UWV issued a letter dated 28 February

2018 provided additional information and provided further documents, including the project plan

eRecognition.

Following the information received by letter dated February 28, 2018, the AP has submitted to the UWV

letter dated 15 March 2018.

In a letter dated 3 April 2018, the UWV responded to the AP's questions of 15 March 2018 and hereby

'risk analysis absenteeism reporter' (hereinafter: the risk analysis).

20. In response to the information received by letter of 3 April 2018, the AP has sent a letter to the UWV

of May 14, 2018 questions asked.

21.

In a letter dated May 25, 2018, the UWV responded to the questions from the AP dated May 14, 2018.

Research report

22.

23.

In the investigation report, the AP found that the UWV in the employer portal

processes personal data about health. Access to the employer portal is obtained by

entering an email address and password. This is a form of one-factor authentication.

It follows from article 13 of the Wbp - now article 32, first paragraph, of the AVG - that a

responsible must take appropriate measures to protect personal data against loss or

any form of unlawful processing. The term 'appropriate' also indicates proportionality

between security measures and the nature of the data to be protected. Given the sensitivity of

the personal data that are processed in the employer portal of the UWV, namely data about

health of workers, accessing the portal via the Internet should be given the

state of the art, to take place by means of at least multi-factor authentication.

24. The UWV has indicated that it has taken measures to prevent unauthorized access to the employer portal, such as conducting annual penetration and security tests and the continuous logging and monitoring of usage. These measures are regarding authentication inappropriate because they cannot provide an adequate level of protection for access

to the application. Because the UWV does not apply multi-factor authentication, nor in any other way has taken appropriate measures with regard to obtaining access to the data in it employer portal, the UWV acts in violation of Article 13 of the Wbp, as it applied at the time.

Legal framework

25. The relevant legal framework is included as Annex 2 to this decision.

AVG

26.

27.

In the investigation report, the AP has found a violation of the standard in Article 13 of the Wbp detected. As of May 25, 2018, the AVG and UAVG are applicable and the Wbp has been withdrawn.

When assessing whether there has also been a violation of the standard from the GDPR, it is important that the standard under the AVG does not materially change materially compared to the standard under the Wbp.

The standard from Article 13 of the Wbp has now been laid down in Article 32, first and second paragraph, of the AVG. The latter article states that the controller, 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,

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

to ensure a level of security. This obligation materially corresponds to the obligation from

Article 13 of the Wbp.

28.

This means that, since the facts under investigation and the relevant circumstances after the conclusion

of the research report have not been changed to date, as of 25 May 2018

violation of article 32, first paragraph, of the GDPR.

View

29. In response to the AP's intention to impose an order subject to periodic penalty payments, the UWV

gave an oral opinion during the hearing on 6 February 2018. In summary, it comes

This view boils down to the fact that the UWV acknowledges that the security of the employer portal does not meet the

requirements

requirements arising from Article 13 of the Wbp and currently Article 32, first paragraph, of the AVG because the UWV

does not apply multi-factor authentication to granting access to the portal.

30. In April 2017, the UWV decided to start implementing eHerkenning level

3/substantial, where multi-factor authentication is applied and thus the violation of Article 13

of the Wbp and currently Article 32, first, of the AVG is abolished. The UWV has when determining

the level of confidence the fact that only health data is shown in the employer portal

processes related to reporting sick or the fact that someone is pregnant.

The nature of the sick report is not processed.

Date

July 31, 2018

Our reference

z2018-02009

31.

32.

33.

34.

35.

36.

The UWV has put forward that it has investigated other solutions, but the connection to
Seeing eHerkenning as the only realistic option to achieve multi-factor authentication. With the
With the introduction of the Digital Government Act (hereinafter: Wdo), it is the intention that all government parties
use the means set out in this Act.
In the implementation of eHerkenning, the UWV is partly dependent on third parties and the UWV runs into difficulties
a number of problems, as a result of which the implementation is taking longer than the UWV had expected
hoped.

Judgement

Assessment framework

In the investigation report, the AP determined that the UWV in the employer portal
processes personal data, including special personal data. This includes name and address
data, BSN, financial data and data about incapacity for work, dismissal and childbirth.
Employers can log in to the portal via the internet by entering an e-mail address and password
feed. This is a form of one-factor authentication 1. From the documents and what has been discussed is at the hearing
shows that this situation has not changed.
Article 32, paragraph 1, of the GDPR stipulates that the controller must take appropriate technical and
must take organizational measures to protect personal data against loss or
unlawful processing. These measures guarantee, taking into account the state of the art
and the costs of implementation, an appropriate level of security in view of the risks posed by the
processing and the nature of the data to be protected.
This means that the person responsible, in this case the UWV, must translate the risks

for the data subject whose personal data are processed in accordance with the reliability requirements
the service that is offered (the employer portal) must comply and that within the field
information security is regarded as the most recent and representative interpretation thereof.
When determining the risk for the data subject, the nature of the personal data and the
nature of the processing matters: these factors determine the potential harm to the individual
data subject in the event of, for example, loss, alteration or unlawful processing of the data. When making
the UWV can use the translation to the reliability level of the employer portal
making the Handbook 'Reliability levels for digital services, a handbook for
government organisations, version 4' of Forum Standardization (hereinafter: the Guide).
37.
Although the use of this Guide is not mandatory, it does provide an assessment framework
government organizations for determining assurance levels for digital services
1 Authentication is the process of verifying whether a user who wants to log in to an application/system is really who
he/she claims to be.

Date
July 31, 2018
Our reference
z2018-02009
which can be assumed to reflect the most recent insights and requirements.
Security standards then provide, after determining the applicable
confidence level, support for taking appropriate measures.2
The AP has investigated whether the UWV has taken appropriate measures with regard to authentication
when logging in to the employer portal. In its investigation, the AP has only focused on the nature of
the personal data to be protected, which translates into a minimum to be used
security level. The assessment in this decision is therefore based solely on the nature of the te

protect personal data. It cannot be ruled out that factors other than the nature of the
personal data require a higher level of security. However, the AP cannot, as explained below
order will come, for or instead of the UWV all relevant - included in Guide version 4
assess factors. It is up to the UWV to include these factors in a risk analysis
determine the appropriate security level.3

Information about a person's health

In Article 4, part 15, of the GDPR, the following definition is given: 'health data
are personal data related to the physical or mental state of a natural person
person, including data on health services provided with which information about his
state of health is given". Under the GDPR, that concept remains unchanged
'health data' should be interpreted broadly: it does not only include the data that a doctor at a
medical examination or medical treatment, but all data that the mental or
affect a person's physical health. For example, it is only given that someone is sick
reported a health detail, even if it says nothing about the nature of the condition.4

The following data is processed in the employer portal: the date of commencement
sick leave, the date of termination of sick leave, sick as a result of pregnancy, childbirth or
organ donation, the date of childbirth and the date of maternity leave.

Given the nature of the personal data, the employer portal therefore becomes data
processes relating to someone's health, which constitutes a special category of personal data such as
referred to in Article 9, paragraph 1 of the GDPR.

Increased risk

The AP has elaborated the security requirements in the Guidelines for the Protection of Personal Data.
The AP indicates that with certain categories of personal data, the consequences of loss or
unlawful processing can be serious. This is the higher or high risk data.
These categories in any case include special personal data.

38.

39.

40.

41.

2 See also CBP Guidelines, Security of personal data, February 2013

3 With regard to the risk analysis by UWV, see marginal number 54 et seq. of this decision

4 Parliamentary Papers II 1997/98, 25 892, no. 3, p. 102

Date

July 31, 2018

Our reference

z2018-02009

42.

In addition, the AP uses the Guide version 45. This Guide gives substance to the
assurance levels based on the eIDAS regulation for digital identifications
trust services6, which came into effect on 1 July 2016 (hereinafter: the eIDAS regulation).
The eIDAS regulation distinguishes three assurance levels of means of authentication: low,
substantial and high. The Guide offers a classification model with which a simplified
risk analysis of the digital service can be made. The most important criterion here is the nature of
the personal data to be protected. Four classes of personal data are distinguished here: class
0, I (basic), II (increased risk) and III (high risk), where data with an increased risk also includes a
require a higher level of security.

43.

The AP has established that the data processed in the employer portal, according to the Handreiking
so-called class II personal data because it concerns special personal data. For
class II data, there is an increased risk.7 From a high risk, as with the so-called class III
data, given the nature of the data processed in the portal, this is not the case.

Multi-factor authentication

44. According to the Guide, there is a minimum reliability level for processing class II data 'substantially' applies.8 Also when answering the question what about this assurance level are appropriate measures as referred to in Article 32(1) of the GDPR the Guidance provides a framework: both for assurance level 'substantial' and confidence level 'high' is, as a type of authentication means, multi-factor authentication required.9

45.

The requirement of multi-factor authentication when granting access to a system in which health data is processed is also endorsed by security standards such as NEN-7510, which provides instructions for applying the Code for information security ISO/IEC 27002 in healthcare:

5 A guide for government organisations: Assurance levels for digital services, version 4, Standardization Forum

6 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market

7 A guide for government organisations, version 4, Standardization Forum, p. 33

8 A guide for government organisations, version 4, Standardization Forum, p. 29. It is possible that UWV after the risk analysis based on all the criteria mentioned in the Guidance version 4, the confidence level is 'high' instead of 'substantial'. The UWV will have to make this assessment itself, see also marginal 54 et seq.

9 A guide for government organisations, version 4, Forum for Standardization, p. 24 – 25. This requirement is laid down in the Annex to the European Commission Implementing Regulation 2015/1502 establishing minimum technical specifications and procedures on the assurance level for electronic identification means in accordance with art. 8(3) of the Regulation (EU) no. 910/2014, on which the Guidance is based.

Date

July 31, 2018

“Health information systems that process personal health information include users' identities

and this should be done through authentication involving at least two factors

become.”10

46.

As an appropriate measure as referred to in Article 32, paragraph 1, of the GDPR, when granting

access to the employer portal can therefore be made using multi-factor authentication.

Now that access to the portal takes place through a form of one-factor authentication, the UWV is acting

contrary to article 32, first paragraph, of the GDPR. UWV has also acknowledged this.

Offender

47. The UWV can be regarded as an offender because it is the controller within the meaning of the GDPR.

The UWV determines the purpose of and means for the processing of personal data: the

employer portal is a service of the UWV and is made available by the UWV to

employers, whereby the purposes of the data processing are determined by the UWV.

The UWV also has the power to end the violation.

The solution of the UWV: eHerkenning

48.

49.

In a letter dated 25 January 2016, the UWV has already announced the violation of Article 32, first paragraph, of the

Wbp recognized. The UWV indicated its intention to use the employer portal

making eHerkenning, which provides for the use of multi-factor authentication in the

providing access to the employer portal.

EHerkenning is a system that offers companies electronic access to the government and

government facilities. Entrepreneurs or employees of an organization can use one

Securely and easily identify a login with different organizations. Government organizations need

not develop their own authentication system, but can connect to the system. The

The development of eHerkenning is a public-private partnership under the direction of the

Ministries of Economic Affairs and Climate Policy and the Ministry of the Interior and Kingdom Relations.

EHerkenning has five different confidence levels. At these confidence levels

connection sought with the three assurance levels distinguished by the eIDAS regulation and the

requirements imposed on the means by that Regulation. The government organization decides for itself

confidence level applied.

50. The UWV has indicated that the introduction of eHerkenning by the UWV should be viewed in the

light of the Wdo that is currently being prepared. The Wdo aims to make it safe and reliable

can log in for Dutch citizens and companies at the (semi-)government. This implements

The Netherlands the EU directive on the accessibility of government websites and apps.11 In anticipation of the

10 NEN-7510 (2017), p. 57

11 https://www.digitaleoverheid.nl/diensten/identification-en-authenticatie/eid/wet-gdi/.

Date

July 31, 2018

Our reference

z2018-02009

Wdo has developed eHerkenning by the government. In due course, the UWV will have to comply with this

eRecognition.

51.

The UWV has indicated that it sees the implementation of eHerkenning as the only realistic solution. The UWV

has investigated possible intermediate solutions, with multi-factor authentication with SMS as the second factor

the most viable and safe alternative option. However, the technical implementation of this would be just

take as long as the implementation of eHerkenning and would also require the implementation of

Delay eRecognition, because this has to be done by the same team. Besides, it wouldn't

be effective and proportionate in order to go through two far-reaching implementation processes in quick succession: this leads to additional administrative burdens for employers and inefficient use of public resources.

Time course/schedule

52. The UWV has indicated that it was already working on connecting to eHerkenning in 2015. For the UWV, however, are the availability of the RSIN (Legal Entities and Partnerships Information number) and the BSN for one-man businesses in the eHerkenning system necessary, because without these numbers the UWV cannot link eHerkenning to its systems. The UWV is for this expansion of the system depends on third parties and has made this expansion a condition for the switch to eHerkenning. In April 2017, the UWV decided to stop the implementation of eHerkenning start because at that moment there is a prospect of linking the RSIN to eHerkenning (87.7% of the employer portal users are identified with RSIN). In its opinion of 21 June 2017 the UWV has indicated that the connection to eHerkenning is expected to be realized in May 2018 to have. In November 2017, the UWV will complete the preliminary investigation. In February 2018, the UWV approved it eHerkenning employer portal project plan adopted and sent to the AP at the request of the AP.

53.

According to this project plan, the UWV is heading for 1 November 2018 as the implementation date, followed by a rollout period of one year during which the users of the portal can switch. At the hearing the UWV has indicated that it now assumes implementation in the fourth quarter of 2018. To It is expected that the BSN will also be added to the system in the second half of 2018. For this group the same implementation date with roll-out period applies. There is also a group of users (0.7%) who do not can use eHerkenning and for which no solution is yet available. The UWV has indicated that if no solution is found, this group will no longer be able to use it from 1 November 2019 creating the employer portal.

confidence level; application Handbook version 4

54.

In 2015, the UWV, on the basis of the Standardization Guide available at the time,

version 312 performed a risk analysis. This version of the guide is based on the European

12 A guide for government organisations: assurance levels for authentication at

electronic government services, version 3, Standardization Forum

Date

July 31, 2018

Our reference

z2018-02009

STORKramwerk. This risk analysis showed that level STORK 3 is appropriate.

The UWV sent the AP this risk analysis on request by letter of 3 April 2018.

55.

56.

57.

Version 4 of the Guide was published in November 2016. This version no longer relies on it

STORK framework but, as shown earlier, on the eIDAS regulation. The UWV has this

However, we see no reason to re-examine the risk analysis of 2015 on the basis of this

of the latest version of the Handbook. In its letter of 25 May 2018, the UWV indicates that in the

risk analysis of 2015 UWV has included the eIDAS system as proposed legislation.

The new version of the Guidance has therefore not given rise to a new one

risk analysis".

According to the eHerkenning employer portal project plan, the UWV has chosen to connect to

eHerkenning level 3. This corresponds to eIDAS level substantial.

The AP notes that the risk analysis of the UWV from 2015 is based on version 3 of the Guide.

The standard from Article 32, paragraph 1, of the GDPR, and formerly Article 13 of the Wbp, prescribes that the

controller or controller when taking appropriate technical and organizational measures

in order to ensure an appropriate level of security, takes into account, among other things, the state of the

technology. This includes, among other things, that a risk assessment that has already been carried out should be reviewed from time to time
must be updated on the basis of the standards applicable at that time. So it had
on the path of the UWV to re-perform the risk analysis already carried out in 2015
using the most recent version of the Guide. Failure to do so runs the risk
the end of the implementation period of, in this case, eHerkenning, may no longer be the case
an appropriate level of security.

58. Although reliability level Stork 3 from version 3 of the Handbook seems to correspond with e-IDAS reliability level substantial from version 4 of the Guide, both versions of the
Guide to various assessment frameworks. As a result, testing against version 4 of the Guide leads
possibly to the conclusion that a higher confidence level must be assumed than the UWV
has done so far on the basis of version 3 of the Guide. Ultimately, this determines the
choice of the measures to be taken to ensure an appropriate level of security
guarantees. The AP cannot provide all relevant information from the Guidance version 4 for or instead of the UWV
assess factors.

Order subject to periodic penalty payments and grace period

59.

It follows from Article 16, first paragraph, of the UAVG, viewed in conjunction with Article 5:32, first paragraph, of the Awb that the AP is authorized to impose an order subject to periodic penalty payments in the event of a violation of Article 32, first paragraph of
the GDPR. Pursuant to Section 5:2(1)(b) of the Awb, the order may be aimed at terminating
the observed violation and the prevention of recurrence.

60. The AP orders the UWV to rectify the violation of Article 32,

first paragraph of the GDPR. This means that the UWV is within the benefit period

must take measures to ensure an appropriate level of security with regard to the granting

of access to the employer portal, where logging in is only possible through an appropriate form of

multi-factor authentication (e.g. by using eHerkenning). Because the UWV determines

of the confidence level for the employer portal has used a meanwhile

outdated version of the Guide, the UWV must reassess the assurance level

determined by performing a risk analysis based on version 4 of the Guide.

61.

62.

63.

64.

Article 5:32a, second paragraph, of the Awb stipulates that a grace period is set 'during

which the offender can carry out the order without forfeiting a penalty'. The term

during which an order can be executed without a penalty being forfeited, must be as short

be made possible. The term must be long enough to be able to carry out the burden.

In view of the above, the AP decides that the UWV must comply with the order no later than October 31, 2019.

to fulfil. The AP has taken the planning into account when determining the beneficiary period

of the UWV with regard to the implementation of eHerkenning and the roll-out period referred to therein

of one year after implementation on November 1, 2018.

Article 5:32b, third paragraph, of the Awb stipulates that the penalty amounts must be in reasonable proportion

to the seriousness of the violated interest and to the intended effect of the penalty. At that last one

It is important that a penalty must provide such an incentive that the order is complied with.

If the UWV does not end the established violation within the benefit period, it will be forfeited

a penalty. The AP sets the amount of this penalty at € 150,000 for each month that the

order has not been (fully) executed up to a maximum of € 900,000. In the opinion of the AP, the
amount of these amounts in reasonable proportion to the seriousness of the violation caused by the violation
interest – the protection of special personal data and the privacy of
involved – and are they also high enough to induce UWV to end the violation.
The AP takes into account the costs associated with the implementation of eHerkenning, as well as the
structural additional costs per year.

65.

The AP requests the UWV in good time before 1 October 2018 to carry out a new risk analysis in which the UWV
assigns a confidence level to the employer portal. This is unaffected by the way
that the AP is authorized to conduct an investigation, including an on-site investigation, if it does so
appropriately prevented.

Operative part

The AP places an order with the UWV for violation of Article 32, first paragraph, of the AVG
periodic penalty payment with the following content:

- The UWV must grant access to the employer portal of a
to provide an appropriate level of security, whereby logging in from that moment on is only possible by means of a
appropriate form of multi-factor authentication. Prior to this, the UWV must fulfill the requirement
redefine confidence level by performing a risk analysis based on version 4
of the Handbook.

-After this period, the UWV forfeits a penalty of € 150,000 (in words:
one hundred and fifty thousand euros) for each month that the order is not (fully) executed up to a maximum

of € 900,000 (in words: nine hundred thousand euros).

The Dutch Data Protection Authority,

On their behalf,

e.g.

mr. A. Wolfsen

Chair

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

decision to submit a notice of objection to the Dutch Data Protection Authority, PO Box 93374, 2509 AJ The Hague,

stating “Awb objection” on the envelope.