Confidential/Registered

UWV

Board of Directors

attn mr. M.R.P.M. Camps

PO Box 58285

1040 HG

AMSTERDAM

Date

May 31, 2021

Our reference

[CONFIDENTIAL]

Contact

[CONFIDENTIAL]

Subject

Decision to impose a fine

Authority for Personal Data

PO Box 93374, 2509 AJ The Hague

Bezuidenhoutseweg 30, 2594 AV The Hague

T 070 8888 500 - F 070 8888 501

authoritypersonal data.nl

Dear Mr. Camps,

The Dutch Data Protection Authority (AP) has decided to inform the Implementation Institute

to impose an administrative fine of € 450,000 on the employee insurance schemes (UWV). UWV has

insufficiently a risk-appropriate level of security guaranteed and safeguarded in the context of

sending group messages via the My Workbook environment. As a result, UWV is in conflict

acted in accordance with Article 13 of the Personal Data Protection Act and Article 32, paragraphs 1 and 2,

of the General Data Protection Regulation.

The AP explains the decision in more detail below. Chapter 1 is an introduction and Chapter 2 contains the facts.

In Chapter 3, the AP assesses whether personal data is being processed, the

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

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

1 Introduction

1.1 Concerned Government Agency

This decision relates to the Employee Insurance Agency (hereinafter: UWV). Since

In August 2016, nine data breaches occurred at UWV that were of a similar nature. The

data breaches all occurred when sending a group message to a group of job seekers.

In doing so, an incorrect (Excel) file with a multitude of sensitive and special

personal data of a varying number of job seekers sent along in the 'My Work folder'

environment of job seekers. The number of job seekers whose data between 2016 and

2018, ranged from 10 to 11,062 people per data breach.

Because in a two-year period, nine similar data breaches had occurred despite that

UWV had indicated that it had taken measures, there was a suspicion that UWV had not taken appropriate measures

technical and organizational measures (as required by law) had been taken to achieve an appropriate

level of security that prevented new similar data breaches.

That is why the AP has started an official investigation. This decision covers the period from 2012 to

through 2018.

1.2 Process flow

On September 4, 2018, a supervisor of the AP contacted the

data protection officer (hereinafter: FG) of UWV. Then AP supervisors have

requested information several times from UWV, to which UWV provided this information. UWV also has

sent further documents to the AP on its own initiative.

On October 31, 2019, UWV was asked to respond to the facts as known to the AP until then.

The UWV responded to that request on 14 and 18 November 2019. In a letter dated March 11, 2021, the AP

sent an enforcement intention to the UWV. To this end also with this letter by the AP in the

given the opportunity, the UWV issued a written opinion on this intention on 8 and 19 April

and the underlying report with findings.

2. Facts

2.1 Duties of the UWV and communication with job seekers

UWV was established pursuant to Article 2, paragraph 1, of the Work and Implementation Organization Structure Act

income (SUWI). UWV is an independent administrative body1 with its own legal personality.2

Within UWV, the WERKbedrijf division is involved in job placement and reintegration. This does

by bringing supply and demand together. The WERKbedrijf focuses primarily on job seekers with

a great distance to the labor market and on employers who want to hire these job seekers.

Persons who want to apply for a benefit on the basis of the Unemployment Insurance Act must register with the UWV

register as a job seeker.3

Werk.nl is a website of the UWV. Since 2007, every jobseeker on werk.nl has a personal

environment that helps him/her to look for a job: My Workbook.4 If a jobseeker has a

benefits, this can be done via My Workbook, including changes, tasks and application activities

passing on and exchanging messages with attachments with UWV.5

UWV can use group messages if the same message is sent to several jobseekers

must send. These UWV messages are placed in the My Workbook environment of jobseekers

justifiably.

2.2 Source system with stored jobseeker data: Sonar

Sonar is the most important source system that WERKbedrijf and municipalities use to find job seekers

to mediate for work by linking job seekers to vacancies at employers.6 The system

contained data on an average of 4,500,000 individuals in the years 2016 to 2018, including

jobseekers, the sick and the disabled.7

Sonar contains 630 data fields containing all kinds of personal data. Not for every one

person, all data fields have been filled in.8 The data in Sonar include names and addresses,

education (level), nationality, BSN, data about physical limitations, psychological and physical

work ability and whether people feel or are too ill to work. As for some of

1 See, among other things, Article 4 paragraph 1 SUWI and the ZBO register of the Dutch government.

2 See article 2 paragraph 2 SUWI and article 4 paragraph 1 SUWI and the ZBO register of the Dutch government.

3 See Article 26(1)(b), (d) and (e) of the Unemployment Insurance Act.

4 See, among other things, file document 98 (Answer by UWV, file "Additional questions AP2110", p. 1).

5 See e.g. file document 120 (Pages website werk.nl 'Manual: Using Workbook').

6 See e.g. file document 6 (Presentation Program Council on UWV applications, p. 2, 3, 6 and 11).

7 See file document 38 (Excel file, answer to question 6 in data breach 1) and file document 98 (Answer by UWV, file

"Additional Questions AP2110", p. 1).

8 See file document 38 (Excel file, answer to question 6 in data breach 1) and file document 81 (Answer by UWV, appendix 1

(file

"Answer to questions AP August 2019", answer to question 9) and annex 4 (file "Question 9 - annex")).

Date

This data may relate to the state of mind or perception of the job seeker who owns an online job

completed the questionnaire.9

Sonar has about 15,000 users. Half of the total number of accounts belongs to WERKbedrijf and

municipalities and the other half is from other divisions within UWV. All users have the option

create and save searches. Users have based on function and associated tasks

access to this data.10

2.3 Group Messages

On July 16, 2012, after data leaks via e-mail, the management of WERKbedrijf

group messaging functionality in Sonar made mandatory for sending group messages to

several jobseekers at the same time.11 This decision was also taken at that time together with the Quick Reference Card “Send Sonar group mail to the workbook” compelling the attention of the executive

employees of UWV.12 A Quick Reference Card is provided by UWV within the WERKbedrijf

used for recording procedures and communicating these to UWV employees

procedures.

Certain actions are required to send a group message or an invitation to a selection via Sonar

jobseekers.13 First of all, an employee of UWV selects a certain group

persons in Sonar and retrieves types of data about them in Sonar. The employee then exports

of UWV this set with data of specific persons from Sonar and stores this exported data

on. This data is then converted into an Excel/csv file. There is no limit on the number

persons whose data can be exported. In addition, the files are not secured,

because, according to the UWV, this would make implementation more difficult.14 This file is then used as a basis

to determine the recipients of the group message.15 The group message passes through the

UWV then with the addressees in the My Workbook environment. This process for spreading

of a group message, UWV describes this in the Quick Reference Card “Sonar Sending group messages

from Sonar to the work folder” (hereinafter: QRC group messages).16

9 See file document 38 (Excel file, answer to question 2 in data breaches 1 to 7) and file document 81 (answer by UWV, appendix 1

(file "Answer to questions AP August 2019", answer to question 3) and appendix 2 (file "Question 3 - appendix")).

10 See, among other things, file document 81 (Answer by UWV, appendix 1 (file "Answer to questions AP August 2019", answer to question

10)).

11 See, among other things, file document 98 (Answer by UWV, file "Additional questions AP2110", p. 3 and appendix 6 (file "29-12

action point list DT", p. 3 under point 4)).

12 See file document 98 (Answer by UWV, file "Additional questions AP2110", p. 2 and appendix 4 (file "28 BV 06 Semi-trailer prohibit Outlook group messages 0406212") and appendix 5 (file "28 BV 06 Decision document prohibiting use of group mail via

outlook")).

13 See file document 66 (Answer by UWV, p. 3).

14 See file document 38 (Excel file, under “Brief description” regarding all data leaks) and file document 81 (Answer by UWV, appendix 1 (file "Answer to questions AP August 2019", answer to question 11)).

15 See file document 81 (Answer by the UWV, appendix 1 (file "Answer to AP August 2019 questions", answer to question 11)).

16 See file document 38 (Excel file, appendix 29 (file "Microsoft Word 97-1003 document" with explanation to answer to question 13

for data leak 6 and 7)), file document 91 (Answer by UWV, appendices 1 to 4).

Date

May 31, 2021

According to UWV, there is a limitation on the number of people when sending a group message
who the message can be sent to.17 Since mid-2013 to date, this number has been limited to 100 to
prevent technical problems in Sonar, improving its operation and stability, and
message traffic runs more smoothly.18 This is stated in all versions of the QRC group messages used
a UWV employee still wants to approach more than 100 people via the My Workbook environment, this
can be requested from Functional Management. Functional Management can do the maximum very temporarily
increase to a larger number of people.19 The QRC also states that group messages can contain attachments
be sent with group messages via Sonar, but it is preferred not to.20
In the period from January 2016 to September 2018, according to UWV, a total of 61,214
group messages sent via the My Workbook environment, with an average of 215 recipients
people per group message.21

2.4 Data breaches related to the group messages

In total, since the beginning of 2016, there have been nine data breaches related to the personal
environment of jobseekers: Mijn Werkmap.22 The UWV has reported eight of these data leaks to the AP.23
Before January 1, 2016, there was no obligation to report data breaches to the AP.
With these data leaks, the Excel file with the export is always out when the group message is created
Sonar added. This caused this file to come up with the export (instead of a message that sent
such as, for example, a vacancy text) in the My Workbook environment of job seekers
justifiably. As a result, the unsecured and consultable file with the individual data could not be accessed
recipients of the message reach all intended recipients.24
The AP has presented the most important facts about the nine data breaches in the table below.25

17 See file document 81 (Answer by the UWV, appendix 1 (file "Answer to AP August 2019 questions", answer to question 11)).

18 See file document 91 (Answer by UWV, appendices 1 to 4).

19 See file document 91 (Answer by UWV, appendices 1 to 4).

20 See file document 91 (Answer by UWV, appendices 1 to 4).

21 See file document 86 (Answer by UWV, appendix 1 ("numbers_messages_ap" file)) and file document 91 (Answer by UWV, appendix 5 (file "numbers_messages_ap")).

22 See, among other things, file documents 8 to 12 and 15 to 21 (data breach (follow-up) reports to AP) and file document 38 (Excel file, answer to

question 6 regarding all data breaches).

23 The ninth data breach was not reported to the AP, because the UWV did not consider it likely that this would pose a risk to the rights and

freedoms of persons. See, among other things, file document 81 (Answer by UWV, appendix 1 (file "Answering questions AP August 2019"), answer to question 8)) and file document 83 (Answer by UWV, answer to question 8).

24 See also file document 45 (Answer by UWV, appendix “Decision memorandum FG investigation”, p. 2).

25 Source of this data: see file document 8, 9, 10, 11, 12, 15, 16, 17, 18, 19, 20, 21, 38, 51, 81, 86 and 98.

Date data breach

Type of data

Number

data subjects

of which the

are data

leaked

Number

those involved

the message

have opened

Date

May 31, 2021

Our reference

[CONFIDENTIAL]

1

2

3

4

8/22/2016

195

9/14/2016

151

9/15/2016

135

9/22/2016

11062

14

20

26

26

5

2/21/2017

189

10

6

3/26/2018

10

7

3/28/2018

90

7

12

Last name, BSN, last occupation,

education level and row ID

Surname, place of residence, date of birth, citizen service number,

first WW day, date on which the WW ends and

of some whether they are sick or at work, that they

cannot be reached by text message or are not digitally skilled

BSN

Last name, postal code, place of residence, e-mail address,

BSN, age, gender, profession (sector),

education (level), first unemployment day and date

on which WW ends, or CV status active or

has expired, number of days of WW on which

job seeker has right, row-ID

BSN, initials, surname, gender, e-mail

email address, age, WORK company location, first

WW day, total score on the online questionnaire and

a short description of obstacles

regarding finding work (such as psychological

or physical work capacity), including for 73

data subjects health data. This

health data does not concern a disease or

medical reports, but for example yes or

someone is too sick to work. From the first WW

day can be deduced that all 189 involved

receiving unemployment benefits (not the amount

of them).

Name, zip code, place of residence, education (level)

and BSN

Last name, zip code,

place of residence, professional sector and BSN

6/41

Date

May 31, 2021

Our reference

[CONFIDENTIAL]

8

8/3/2018

2503

70

Surname, gender, date of birth, citizen service number,

telephone number, level of education, last profession,

last employer, categories

driver's license, oral and written skills

Dutch, first, second and third

professional sector, registration/mediation profession,

available hours per week, hours still working,

first WW day, maximum last day of WW

benefit, age group based on first unemployment benefit

day, indication, whether there is an exemption and the row

ID.

9

9/5/2018

996

9

Last name and row ID

2.5 Policy within UWV

Within UWV, a policy had been drawn up from at least 2016 to reduce risks when processing

to detect personal data at an early stage and to deal with it on the basis of a careful risk assessment,

where risks are neutralized or explicitly accepted by a director. Also serves

UWV register the (outcomes of) risk assessments based on the policy.26

At least from 2016 up to and including 2020, policy had also been drawn up within UWV to address technical and

implement and maintain organizational security measures in a risk-driven manner

monitor, evaluate and adjust.27

2.6 Practice within UWV

2.6.1 Weighing risks in practice

The AP has asked UWV several times whether and, if so, which risk analyzes have been carried out to determine the

protect personal data when sending group messages.28 How and what risks UWV

weighed up precisely, partly in response to the data breaches that occurred, to determine whether

personal data when sending group messages via the My Work folder environment is sufficient

are insufficiently secured, the UWV did not mention.29

In its answers, UWV does not appear to provide an unequivocal and even sometimes contradictory picture of the

(periodically) performing risk analyzes with regard to the security of personal data in the

sending group messages via the My Workbook environment. In any case, UWV has stated that it

26 See appendix 1 page 25 for the exact parts of the UWV policy documents.

27 See appendix 1 page 25 for the exact parts of the UWV policy documents.

28 See, among others, file document 27 (Letter to UWV, p. 4-5) and file document 69 (Letter to UWV, question 12) and file document 93 (E-mail to UWV).

29 See, among other things, file document 38 (Excel file, answer to 11 under data leaks 1 to 4) and file document 81 (Answer by UWV, Appendix 1
(file "Answer to questions AP August 2019", answer to question 12)) and file document 98 (Answer by UWV, file "Additional Questions AP2110", p. 2).

did not conduct a risk analysis prior to the 2012 decision to go group messaging
send via the My Workbook environment. The UWV has stated a number of times that from 2016 to
and with the last data breach in 2018 in the context of the security of personal data when sending
of group messages via the My Workbook environment has performed risk assessments. From the
answers from UWV and submitted documents, however, it is not clear how these risk assessments are
and what risks have been weighed up at any point in that period. UWV also has the
risks not regularly weighed.30

2.6.2 Measures, control and adjustments in practice

UWV stated in the data breach reports to the AP of the second and third data breach that they are investigating
was whether technical measures are possible to prevent these data leaks.31 In the notification of the
fourth data breach at the AP, UWV indicated that it was investigating whether it was possible to place “such
files” in the My Workbook environment.32 UWV stated in the data leak reports to the AP
of the third and fourth data breach at the end of September 2016 that the employee who made the mistake

this had been addressed by the management and that awareness was being looked at.33

After the first four data leaks in 2016, UWV decided to take organizational measures.

On 28 September 2016, the UWV first decided on temporary organizational measures.34 And although

UWV has stated that these temporary measures are still in force, following a decision by the UWV

District managers consultation (DMO) of UWV that the temporary measures taken on September 28, 2016

was decided, were replaced in October 2016 by other organizational measures. Furthermore, the

AP determined that UWV has drawn up the “Guideline for safe communication at WERKbedrijf” and that the

intention to investigate the possibilities of taking technical measures

UWV has been implemented. In addition, the AP has concluded that the

organizational measure(s) prior to the fifth data breach has not been checked nor

evaluated by UWV.35

After the fifth data breach (February 21, 2017), UWV subsequently decided to take further organizational measures

measures with regard to sending group messages via the My Workbook environment,

namely by raising awareness. UWV did this through workshops and a few visits

to districts. The UWV then decided not to take any technical measures. By the way, the after 20

October 2016 organizational measure(s) in force regarding the sending of

group messages via the My Workmap environment also not prior to the sixth data breach by UWV

neither checked nor evaluated.36 UWV's statement that these measures did check and

evaluated, UWV has not substantiated with documentation.

30 See appendix 1 pages 26 and 27 for the exact answers of the UWV.

31 See file documents 9 and 10 (Data leak reports).

32 See file documents 11 and 12 (Data breach (follow-up) reports).

33 See file document 10 (Data leak notification) and file documents 11 and 12 (Data leak (follow-up) reports).

34 See appendix 1 pages 28 and 29 for the exact measures of the UWV.

35 See appendix 1 pages 30 to 34 for the exact measures and statements by the UWV.

36 See appendix 1 pages 33 to 35 for the exact measures and statements by the UWV.

Date

May 31, 2021

Our reference

[CONFIDENTIAL]

After the seventh data breach (March 28, 2018), UWV has decided to take several organizational measures. However, UWV and WERKbedrijf have not checked as such whether these measures actually work have been introduced.37 Apart from two measures38, the UWV also has no documents or a further one substantiation provided on the basis of which it can be determined whether the organizational measures are secured in documentation and when they are implemented.

After the eighth data breach (August 3, 2018), UWV has decided to introduce a technical measure, namely blocking the possibility of adding, among other things, Excel files when sending group messages via the My Workbook environment to prevent data breaches to prevent. This technical measure was taken by UWV in December 2018, so far after the ninth data breach implemented.

The above facts cover the period from 2012 to 2018. This decision and the investigation of the AP refer only to this period. The UWV does have the following in its view declared for the period after 2018.

UWV has stated that in the process of sending group messages in the My Workbook environment in addition to the technical measure, which has the specific risk of sending Excel lists removed, there has also been an active effort to raise awareness among (new) employees in the implementation who have frequent (digital) contact with jobseekers for the performance of their duties. In addition process descriptions and Quick Reference Cards (QRCs) are now being produced annually within WERKbedrijf evaluated and adjusted if necessary.

In addition, at the end of 2018, the DPO conducted an investigation on behalf of the Board of Directors of UWV prepared in response to the eighth data breach and a report of findings. Specific to it

mitigating the risks of sending group messages in the My Workbook environment, it states
FG investigation that the technical measure uploading Excel files to the My Workbook
environment impossible, an effective measure is to prevent this type of data breach.
Partly as a result of the FG investigation, UWV WERKbedrijf has further awarded the contract to KPMG
given to conduct a broader investigation of the source system SONAR. This is to determine where the
vulnerabilities and risks are located in technical, process and organizational areas,
whereby the already existing organizational and technical measures have also been evaluated (check-
phase). In 2020, this research resulted in four advisory reports with 77 recommendations. It
advisory report on privacy has largely been made public by UWV.39
In response to the advisory reports, the large-scale improvement project SONAR IB&P was started in 2020,
which aims to address the findings of the study and SONAR's IB&P risk level
to be greatly reduced (act->plan->do phases). In that context, UWV will take an extra technical measure
37 See appendix 1 pages 35 to 41 for the exact measures and statements by the UWV.
38 The 'Step-by-step plan for the safe sharing of personal data', which the UWV communicated to employees on 1 May 2018.
Also had
UWV extended the QRC group messages with the passage about cleaning (Excel) files and the 4-eyes principle.
39 See https://www.uwv.nl/overuwv/Images/bijlage-1-bij-besluit-wob-request-onderzoeksrapport-sonar-privacy.pdf.

implement. The export functionality from SONAR for implementation collaborators, except for a few
authorized employees, will be closed.
According to UWV, the recommendations from the KPMG study also aim to improve the
risk management process, including the Plan-Do-Check-Act cycle (hereinafter: PDCA cycle). Of

this improvement in risk management and the implementation of controls will make it
WERKbedrijf the growth in the implementation of the PDCA cycle - and thus ensure that there
appropriate technical and organizational measures have been and will be taken – continue.

3. Legal Review

3.1 Processing of personal data

As of 25 May 2018, the General Data Protection Regulation (GDPR) is applicable.40 Given the
facts in this investigation took place between 2012 and 2018, the AP will comply with both the Protection Act
personal data (Wbp) and the AVG tests.

The concept of personal data is defined in Article 1, under a, of the Wbp and Article 4, part 1, of
the GDPR. Article 16 of the Wbp defines personal data about health as special
personal data identified. In Article 9, the GDPR also marks data about health as
special personal data.

Personal data within the meaning of the Wbp and the AVG are all information about an identified or
identifiable natural person. Sonar includes data about natural persons such as
names, addresses, the BSN and other data. With this data, the registered in Sonar
natural persons, including job seekers, are identified directly or indirectly. contains sonar
therefore personal data within the meaning of Article 1, under a, of the Wbp and Article 4, part 1, of the AVG.

Sonar also includes data about physical limitations and the psychological and physical
work ability of persons. Sonar also states whether people feel too ill to work. On
pursuant to article 16 of the Wbp and article 4, section 15, of the GDPR, this is information about the
health.

From the above it follows that UWV when sending group messages via the My Workbook environment
personal data, including the BSN and health data, processed within the meaning of the Wbp and
the GDPR.

40 On that date, the Personal Data Protection Act (Wbp) was repealed pursuant to Article 51 of the UAVG.

3.2 Controller

The concept of controller or controller is defined in article 1, under d, of the Wbp and article 4, part 7, of the GDPR. In the case of independent administrative bodies at national level, the body charged with the tasks and exercise of powers for which the data are processed, as the controller are to be noted.

As stated in section 2.1, the UWV was established on the basis of a law, namely the SUWI. UWV is one independent administrative body of the central government with its own legal personality. As above In the case of independent administrative bodies at central government level, the body charged with the duties and exercise is stated of powers for which the data are processed, to be regarded as responsible. UWV has both legal and factual control over the processing of personal data are collected in the context of sending group messages through the workbook.

On the basis of the above, the AP designates UWV as the (processing) controller as referred to in Article 1, under d, of the Wbp and Article 4, part 7, of the AVG for the processing of personal data in the context of sending group messages via the workbook.

3.3 Security of the processing of personal data

3.3.1 Legal framework

From September 1, 2001 to May 25, 2018, with regard to the security of the processing of personal data Article 13 of the Wbp. The security obligation extends to all parts of the data processing process. The term 'appropriate' implies that security is in is in accordance with the state of the art. This is primarily a professional question ethics of persons charged with information security. The standards of this ethic are set out in this

provision with a legal capstone, in the sense that it is a legal obligation for the

responsible person is connected. The term 'appropriate' also indicates a proportionality between the

security measures and the nature of the data to be protected. For example, as the data

are of a more sensitive nature, or the context in which they are used poses a greater threat to the

mean privacy, stricter requirements are imposed on the security of the data.

The European directive on the basis of which, among other things, Article 13 of the Wbp has been drawn up considers under

others the following with regard to the security of the processing of personal data: “that the

principles of protection (…) should be reflected in the obligations imposed on persons, public authorities,

obligations are imposed on companies or other bodies that carry out the processing, in particular

relate to data quality, technical security, notification to the supervisory authority

authority and the circumstances in which the processing can be carried out (…)”.41 It also mentions at

with regard to the security of the processing of personal data considered: “that the protection of the

rights and freedoms of data subjects in relation to the processing of personal data both at design and

41 See Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data

personal data and on the free movement of that data, recital 25. Underlining of the AP.

Date

May 31, 2021

Our reference

[CONFIDENTIAL]

requires appropriate technical measures when carrying out the processing, in particular to ensure security

and thus prevent any unauthorized processing; (…)”.42

In a case involving access to electronic medical records, the Dutch DPA has regard

of taking security measures in the context of Article 13 of the Wbp as follows:

“A controller may only proceed to take purely organizational measures if he can demonstrate this

it is not possible to take appropriate technical measures. This must then be compensated with extra

organizational measures and monitoring compliance with them".43

In 2013, the Dutch DPA has issued guidelines with regard to security in order to implement Article 13 of the Wbp of the processing of personal data (hereinafter: CBP guidelines).44 When drawing up the CBP guidelines, a connection has been sought with ISO27001. The guidelines state as necessary preconditions to ensure a continuous appropriate level of security for processing to obtain and guarantee personal data as required by law: "take measures based on risk analysis, applying security standards and embedding it in a plan-do-check-act cycle".

The CBP guidelines state about this PDCA cycle: "After establishing the reliability requirements, the responsible measures with which he guarantees that the reliability requirements are met. Thereafter the person responsible checks whether the measures have actually been taken and are having the desired effect. The total reliability requirements, measures and control are regularly evaluated and adjusted where necessary, so that a continuing appropriate level of security is achieved".45

Like ISO27001, the CBP guidelines (as part of the PDCA cycle) also prescribe that the controller takes security measures based on a risk analysis, in which he determines the identifies threats that could lead to a security incident, the consequences it security incident and the probability that these consequences will occur. When inventorying and assessing the risks, the consequences that those involved may experience are particularly relevant unlawful processing of their personal data. These consequences can, depending on the nature of the processing and of the processed personal data, include stigmatization or exclusion, damage to health or exposure to (identity) fraud.46

Article 32 of the GDPR contains the requirements regarding the security of the processing of personal data included. The risk should be taken into account when determining appropriate measures for the rights and freedoms of individuals.47

Recital 83 of the GDPR states with regard to ensuring the security of the processing of personal data and the assessment of the risks: "In order to ensure security and prevent the

42 See Directive 95/46/EC, recital 46. Underlining of the AP.

43 See e.g. case Z2003-0145, p. 3.

44 See CBP guidelines: security of personal data, https://wetten.overheid.nl/BWBR0033572/2013-03-01.

45 See CBP guidelines: security of personal data, https://wetten.overheid.nl/BWBR0033572/2013-03-01.

46 See CBP guidelines: security of personal data, https://wetten.overheid.nl/BWBR0033572/2013-03-01.

47 See also recital 75 of the GDPR.

processing infringes this Regulation, the controller or processor should inform the

assess risks inherent in processing and take measures, such as encryption, to mitigate those risks. That

measures should ensure an appropriate level of security, including confidentiality

taking into account the state of the art and the implementation costs against the risks and the nature of the protection

personal data. When assessing the data security risks, attention should be paid to risks that

occur during personal data processing, such as destruction, loss, alteration, unauthorized

provision of or unauthorized access to the data transmitted, stored or otherwise processed, or

accidental or unlawful, which can lead in particular to physical, material or immaterial damage."

Finally, in 2007 the Decree on Information Security for the Civil Service (hereinafter: VIR) came into force

48 In the 2014 Administrative Statement on Information Security, the UWV declares that it will go to VIR

use.49 With regard to terms used in the VIR, the following is indicated: "The conceptual framework of the

Code of Information Security (ISO17799:2005) has been adopted in this regulation".50 The PDCA cycle from

ISO17799:2005 has since been included in ISO27001.51. This standard contains a number of steps that

should be performed. The steps form a so-called Plan-Do-Check-Act cycle (hereinafter:

PDCA cycle) to respond to (constantly changing) threats to the information.52

Article 4 VIR specifies the responsibilities of line management. In general

explanation to the VIR, the following is included about article 4 VIR: “It was deliberately chosen to include article 4 formulate terms of the Planning and Control cycle, in accordance with regular business operations. (…) Information security itself takes place via the quality circle of Deming (PDCA cycle)”.53 The article-by-article explanatory notes to the VIR state in addition with regard to article 4: “For the effectuation of information security, work is done via the Plan Do Check Act cycle (...). After determining what is necessary (reliability requirements), measures are taken and checks whether those measures have the desired effect (check). This check can immediately lead to adjustments in the measures. The total of requirements, measures and control may also be in need of revision (evaluation). It proper completion of this quality circle ensures an adequate level of security at all times”.54

3.3.2 Assessment

It follows from both Article 13 of the Wbp and Article 32, first and second paragraph, of the AVG that the controller must take appropriate technical and organizational measures to ensure a risk-based security level of the processing of personal data guarantee/guarantee. These provisions aim to safeguard the same (legal) interests and there is none (substantial) material change to the regulations on this point.

To ensure a risk-appropriate level of security for the processing of personal data guarantee/ensure, a controller should thus analyze risks, appropriate

48 Government Gazette 28 June 2007, no. 122. https://zoek.officielebekendmakingen.nl/stcrt-2007-122-p11-SC81084.html.

49 Government Gazette 2014, 15447, https://zoek.officielebekendmakingen.nl/stcrt-2014-15447.html.

50 Government Gazette 28 June 2007, no. 122, p. 12.

51 ISO/IEC 27001:2013 chapters 6 to 10.

52 See e.g. ISO/IEC 27001:2013, chapters 6 to 10 and ISO/IEC 27001:2017.

53 Government Gazette 28 June 2007, no. 122, p. 12.

54 Government Gazette 28 June 2007, no. 122, p. 15-16.

take measures and evaluate them. These steps form the preconditions for a continuous

guarantee an appropriate level of security of the processing of personal data in line with the law,

namely by embedding it in a plan-do-check-act cycle (PDCA cycle). This cycle is in line with the

procedure referred to in Article 32(1)(d) of the GDPR, namely a procedure for op

periodically test, assess and evaluate the effectiveness of the technical and

organizational measures to secure the processing. Also the VIR, to which the UWV adheres

has conformed to, is based on ISO27001 and prescribes a PDCA cycle. This general

accepted security standard is also taken into account by the AP in this case. The AP works the

different steps of the PDCA cycle in more detail below.

Weighing up risks to persons prior to determining measures

The starting point that is performed in the context of securing processing

personal data is an assessment of the risks of that processing. It is determined on that basis

what measures are necessary to counter these risks.

This follows from the Wbp and the GDPR and their explanation when considering the data security risks

attention should be paid to risks that arise in the processing of personal data. As

unauthorized disclosure of or unauthorized access to processed data. When taking inventory

and assessing the risks, the consequences that people may experience are particularly relevant

unlawful processing of personal data. As the data becomes more sensitive,

or the context in which they are used pose a greater threat to privacy

mean, stricter requirements are set for the security of personal data.

When sending group messages via the My Workbook environment, as stated in section 2.4,

there has been repeated (accidental) unauthorized disclosure or unauthorized disclosure

access of processed personal data of jobseekers. The UWV is therefore expected to,

in order to arrive at a security level tailored to the risks, continuously inventories and

that could lead to a security incident. The UWV existed from at least 2016

policy to detect and address risks in the processing of personal data at an early stage

based on a careful risk assessment. The VIR also requires the UWV to make an explicit risk assessment

determining appropriate security measures.

As the AP concluded in section 3.1, UWV processes a multitude of different

personal data of a highly sensitive nature, including data about the health of individuals

and the BSN. In the period from 2016 to 2018, the UWV processed data on an average of 4,500,000

persons. Job seekers, sick and disabled people who are legally obliged to register with

UWV and must therefore provide their personal data, must be able to trust that UWV

properly weighs the risks that these persons run. The consequences of a

security incident with regard to the personal data that UWV processes can be serious for

a large group of people. For example, it may not be sufficiently secure for the processing of these

personal data lead to stigmatization or exclusion. Now that UWV also processes the BSN, which is included in the

in practice considerably facilitates the linking of different files, exists for persons

whose data is in Sonar an additional risk of threat to privacy.

The UWV policy contains measures, including an explicit risk assessment as part of a

PDCA cycle. Contrary to this policy, it appears that UWV responds to the

sending group messages via the My Workbook environment gives a contradictory picture about it

performing such risk analyzes with regard to the security of personal data. UWV

has in any case stated that prior to the decision in 2012 to only send group messages

sending via the My Workbook environment no risk analysis has been carried out. Subsequently, UWV stated that from 2016 up to and including the last data breach in 2018, they personal data when sending group messages via the My Work folder environment performed risk assessments. However, it is not clear from the answers of the UWV and submitted documents showed how UWV has made these risk assessments and what risks are involved at any given time in that period have been considered and how the possible consequences for job seekers have been considered. For insofar as UWV is of the opinion that the proposed measures of October 201655 do require a risk assessment contains, the AP notes that there is no weighing of risks in the sense of the (interpretation of the) law. to take. It only contains a proposal for measures without further substantiation. It also shows this document does not state that risks to individuals have been taken into account when proposing measures. Stronger still, UWV only talks about risks that UWV itself runs in its customer communication. Right at one organization such as UWV, which processes so much special and sensitive personal data of so many people, and the consequences for them when sending group messages via the My Workbook environment could be far-reaching, is not taking into account or insufficiently taking into account the risks for job seekers extra careless when determining security measures.

Based on the above, the AP concludes that UWV with regard to the meeting of security measures in the context of sending group messages via the My Workbook environment the risks for job seekers, which, given the sensitivity of the data processed by the UWV can be far-reaching, at least in the period from 2012 up to and including 2018 not/sufficiently mapped has brought. As a result, UWV does not have a security level that is sufficiently geared to risk guaranteed and guaranteed.

Taking technical and organizational measures

After mapping and weighing the risks for individuals of the processing of personal data the established measures must then be implemented and carried out. Both article 13 of the Wbp as well as Article 32, paragraph 1, of the GDPR oblige the controller to take technical and organizational measures to ensure the security of the processing

to safeguard personal data.

Section 2.6 shows that the UWV only has organizational measures until December 2018

implemented in the context of sending group messages via the My Workbook environment every

to ensure the security of the processing of personal data. An example of one

55 See appendix 1 page 30.

organizational measure, the message where employees are called is preferably none

send attachments with group messages via Sonar. The measure regarding a restriction on the

number of job seekers to whom the message can be sent further, as UWV itself states,

to prevent technical problems in Sonar that improve its operation and stability and

messaging runs smoother. This is therefore not for the security of the processing

to safeguard personal data. This limitation only applies to the number of recipients of a message,

but does not limit the number of jobseekers whose personal data can be processed by UVW

sent. Moreover, the limitation to 100 addressees could be circumvented by requesting it

to do with Functional Management. In five out of nine data breaches, the same group message has been sent to more than

100 jobseekers sent at once via the My Workbook environment.

On October 20, 2016 (after the fourth data breach), the UWV decided to conduct an investigation in the short term.

start to the possibility of taking technical measures, including the technical

make it impossible to attach Excel files to a workbook message. It still has until after

the eighth data breach lasted in September 2018 before the UWV then decided to take action

a technical measure, namely blocking the possibility of adding, among other things

Excel files when sending group messages via the My Workbook environment. However, it turns out

UWV only in December 2018 (well after the ninth data breach on September 5, 2018 and well after the 2016 announced investigation into the introduction of technical measures) has proceeded to the three decision taken months earlier to actually implement it. Taking this technical measure was therefore possible.

Apparently, the data leaks were not an urgent reason for the UWV to carry out the investigation that was suggested in 2016 to the possibility of implementing technical measures as soon as possible. By not (also) implementation of a technical measure, the UWV has insufficiently geared it to the risk security level guaranteed and thus accepted a risk of data leaks for more than two years with a lot of personal data concerning a large group of citizens.

Checking and adjusting measures

Technical and organizational security measures are based on both the Wbp and the GDPR ensure a level of security appropriate to the risk. In any case, it is necessary for this to check whether the measures have been implemented, are correctly applied or carried out and what the effect of the measures is on the initially identified risks. Based on this check of the measures, it is then determined whether the measures are still appropriate to the risk guarantee a level of security or whether additional measures are required.

Within UWV, from at least 2016 up to and including 2020, there will be a policy to implement measures check and if necessary adjust as part of a PDCA cycle. However, UWV reports that UWV does not have a generic policy in which it checks whether UWV-central measures are in place implemented in practice by the responsible division(s) and that regional offices to some level to give their own interpretation to central policy. UWV also reports that there are no There is a formally protocolized procedure within UWV within which there is a central level

checked whether such agreed organizational and process measures are being followed
carried out, because that would be impracticable given the size of the organization and the quantity
decisions made by the UWV.
The UWV also indicates that it has not checked whether measures were taken as a result
of data breaches have actually been introduced. In addition, the UWV has entered into force after October 20, 2016
being organizational measure(s) prior to the fifth (2017) and sixth (2018) data breach
neither checked nor evaluated. Finally, UWV has not demonstrated that it has at any time
checked whether the organizational measures that applied prior to the eighth data breach (2018)
have been introduced. The UWV has also not evaluated these organizational measures.
As concluded earlier, the consequences for job seekers are insufficiently secure sending
of group messages through the workbook providing. Especially with an organization like UWV, which is so sensitive
and processes special personal data of so many persons, it is necessary to check whether
measures have actually been (correctly) implemented and to evaluate and where necessary adjust them
to fit. Job seekers and others who are legally obliged to register with UWV and for that
must provide their personal data, must be able to rely on UWV measures
checks, evaluates and, if necessary, adjusts.
Based on the above, the AP concludes that the UWV has implemented the security measures in the
within the framework of sending group messages via the My Workbook environment does not/sufficiently
checked and evaluated, as a result of which the UWV does not provide a security level that is sufficiently geared to the risk
has guaranteed and guaranteed.

3.4 UWV view and AP response

In this section, the AP briefly summarizes the UWV's view, followed by the AP's response.
The UWV first of all notes that it regrets that the
different phases of the PDCA cycle. The UWV greatly appreciates the AP's findings and is firmly committed to them
to improve this process.

3.4.1 Opinion on factual findings

UWV is of the opinion that the analysis of the eighth data breach does show that the eighth data breach and the directly affected

measures have been both analyzed and evaluated by UWV, whereby measures are also proposed.

The AP notes that UWV has indeed analyzed and evaluated the eighth data breach, but

this analysis does not show that UWV processes personal data in the context of sending

of group messages via the My Workbook environment on its own. The evaluation of a

loose data breach is insufficient implementation of a risk-based security level with associated

PDCA cycle. In addition, it cannot be deduced from the analysis that UWV immediately took a measure.

The UWV has discussed the introduction of the technical measure, but this measure is only new

entered later. In addition, the AP considers it necessary to evaluate measures that have just been introduced

not meaningful.

UWV does not refer to the findings that it indicated in August 2019 that the WERKbedrijf is an external

would investigate the export functionality from Sonar and the sending of group messages via

the workbook.

The AP has not included UWV's plan to have an external investigation carried out as a fact

because this was only an intention of UWV. In addition, this intention does not refer to the period from

the established violation. The AP has, however, mentioned this research in paragraph 2.6 of this article

decision.

3.4.2 View of the legal framework and the assessment

The standard that a controller may only proceed to take purely organizational measures if he can

demonstrate that it is not possible to take appropriate technical measures, according to the UWV, does not follow sufficiently from the CBP
security guidelines from 2013, a CBP case56 and the other sources cited in the report.
The AP does not follow this view of the UWV. First, the AP has not only referred to a CBP case, but also to Directive 95/46/EC of 24 October 1995 on the protection of natural persons in relation to the processing of personal data and the free movement of such data, recitals 25 and 46. Secondly, both Article 13 of the Wbp and Article 32 of the AVG that the controller must take appropriate technical and organizational measures.
Technical and organizational measures must be taken cumulatively. The standard in Article 13 of the Wbp and Article 32 of the AVG is thus sufficiently clear, according to the AP. UWV does not have any further argued that it could limit itself to taking only organizational measures, as it was not possible to take appropriate technical measures. Such a point of view would also have been unsustainable, now that the UWV ultimately had a technical one in December 2018 measure has been implemented.
The fact that not all measures were equally effective and that incorrect assessments may have been made is possible in optics of the UWV, it cannot be concluded that no or insufficient implementation has been done appropriate measures. And from the mere fact that there has been some time between the moment of evaluation and the implementation of the technical measure, according to UWV, based on the findings, it cannot be concluded that from the eighth data breach no or insufficient implementation of appropriate measures has been taken, if due to inadequate risk management.
The AP does not follow this view of the UWV and motivates this as follows. The AP has assessed in its entirety whether UWV has a security level tailored to the risk for the relevant processing guaranteed and guaranteed. The fact that the UWV has taken some organizational measures does not detract to the conclusion that UWV has insufficient risk analyses, technical measures and controls executed. As the UWV itself states, this means that the security measures are ineffective

56 https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/arbodienst-handelt-niet-conflict-met-wbp-%C2%A0

Date

May 31, 2021

Our reference

[CONFIDENTIAL]

goods. In addition, the UWV only recommended after the eighth data breach (3 August 2018) to use a
to take a technical measure, while it had already been decided in October 2016 in the District Manager meeting
in the short term the possibility of technical possibilities had to be explored. In this
In the intervening period of almost 2 years, the UWV thus failed to carry out this investigation.
The UWV is also of the opinion that an evaluation has taken place after the eighth data breach. Based on view
UWV therefore does not track the duration of the observed violation above. According to UWV, after the eighth
data breach, an appropriate level of security has been applied.
The AP agrees with UWV that the eighth data breach has been evaluated. However, this evaluation only includes one
data breach. The AP would like to emphasize once again that the UWV does not follow the measures taken periodically
fully evaluated and also failed to sufficiently analyze the risks in advance. The FG
moreover, the investigation only took place from November 2018 and the technical measure has been implemented by UWV
introduced December 2018. The AP therefore does not follow the view that UWV from the eighth data breach
(August 3, 2018) has guaranteed and safeguarded a risk-aligned level of security.
In retrospect, with today's knowledge, according to UWV, the process was not sufficiently followed and there is not enough
documented. The UWV does note that the findings do not show that no interpretation has been given at all
to the different phases of the PDCA cycle or in the entire period from 2012 to the end of 2018.
The AP agrees that the findings do not show that the
different phases of the PDCA cycle, but notes that this has not been sufficiently implemented.
What the UWV has documented shows that only the deadlock was taken into account
of the UWV systems where the risks for those involved were not mentioned. UWV has further
some organizational measures have been taken, but not the necessary (and technical) measures. All of this

resulting in an insufficiently appropriate level of security.

3.5 Conclusion

The AP comes to the conclusion that the UWV does not provide sufficient security level appropriate to the risk guaranteed and guaranteed in the context of sending group messages via the My Workbook environment. As a result, there was a continuous violation in which UWV in the period from 2012 up to and including 24 May 2018 acted contrary to Article 13 of the Wbp and from 25 May 2018 to December 2018 has acted in violation of Article 32, first and second paragraph, of the GDPR.

4. Fine

4.1 Introduction

UWV has acted in violation of Article 13 of the Wbp and Article 32, first and second paragraph, of the AVG. The AP uses its power to impose a fine on the UWV for the established violation for the period from 1 January 2016 (start of AP's power to impose fines) to December 2018. Given the seriousness of the violation and the extent to which this can be attributed to UWV, the AP considers the imposition of a fine due. The AP motivates this in the following.

Given that in this case there is a continuous violation that has both the Wbp and the AVG occurred, the AP tested against the substantive law as it applied at the time when the behavior took place. In this case, that is both article 13 of the Wbp and article 32, first and second paragraph, of the GDPR. These provisions aim to safeguard the same legal interests and there is no (substantial) material change to the regulations on this point. Given that the center of gravity of the offense is located at the time of the Wbp, the AP sees reason in this case to link up with the 'Fining policy rules Dutch Data Protection Authority 2016'.

4.2 Penalty Policy Rules of the Dutch Data Protection Authority 2016

In this case, the AP applies the 'Fine Policy Rules of the Dutch Data Protection Authority 2016' (Financial Policy Rules) for the interpretation of the authority to impose an administrative fine, including determining of the level thereof.57 In the Fining Policy Rules, a categorization and bandwidth has been chosen system.

Violation of Article 13 of the Wbp is classified in category II. Category II has a penalty bandwidth between €120,000 and €500,000. Within the bandwidth, the AP sets a basic fine. As a starting point applies that the AP sets the basic fine at 33% of the bandwidth of the violation linked to the violation fine category.58 In this case, the basic fine is set at € 245,400.

4.3 Fine amount

The AP adjusts the amount of the fine to the factors referred to in Article 6 of the Penalty policies, by lowering or increasing the base amount. It is an assessment of the seriousness of the offense in the specific case, the extent to which the offense can be imposed on the offender and, if there is reason to do so, other circumstances such as the (financial) circumstances in which the offender finds himself.

57 Policy rules of the Dutch Data Protection Authority of December 15, 2015, as last amended on July 6, 2016, with regard to imposing administrative fines (Fine Policy Rules of the Dutch Data Protection Authority 2016), Stcrt. 2016, 2043.

58 Fining policy rules, p. 10-11.

4.3.1 Severity of the Violation

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. When determining the risk for the data subject include the nature of the personal data and the scope of the processing important: these factors determine the potential harm to the individual involved in, for example loss, alteration or unlawful processing of the data. As the data becomes more sensitive character, or the context in which they are used pose a greater threat to the personal mean privacy, stricter requirements are imposed on the security of personal data. The AP has concluded that UWV does not sufficiently have a security level geared to risk guaranteed and guaranteed in the context of sending group messages via the My Workbook environment.

With regard to the nature of the data, the AP has established that UWV contains a multitude of processes various personal data of a highly sensitive nature, including data about the health of persons and the BSN. Jobseekers, the sick and the disabled who are legally are obliged to register with UWV and must provide their personal data for this, must can be confident that the UWV properly weighs the risks that these persons run.

The impact of a security incident with the personal data that UWV processes can be significant for a large group of people. For example, it cannot sufficiently secure this personal data lead to stigmatization or exclusion. Now that UWV also processes the BSN, which in practice is a link of different files considerably facilitated, there exists for persons whose data in Sonar poses an additional threat to privacy.

In addition to the sensitive nature of personal data, the UWV processes data from a great many citizens. UWV processed data in Sonar in the period from 2016 to 2018 on an average of 4,500,000 persons. All of these people were at risk due to the inadequate security level of UWV. Moreover, UWV has already leaked personal data on several occasions. Out of a total of 15,331 persons, UWV leaked data when sending group messages via the workbook. Finally the AP notes that the violation lasted 2 years and 11 months. The AP considers this very serious.

In view of the above, the AP sees reason to, based on the degree of seriousness of the violation

to impose a fine on UWV and to increase the basic amount of the fine to € 450,000.

4.3.2 Culpability

According to Article 6, paragraph 2, of the Policy Rules, the AP takes into account the extent to which the violation can be attributed to the offender. If the violation was committed intentionally or the is the result of seriously culpable negligence as referred to in Article 66(4) of the Wbp assumed that there is a considerable degree of culpability on the part of the offender.

According to the parliamentary history of 'seriously culpable negligence' as referred to in Article 66, paragraph 4 of the Wbp if “the violation is the result of seriously culpable negligence, that is to say

is the result of gross, considerably negligent, negligent or injudicious conduct.”59 In this context it is noted that “acting” as referred to above also includes an omission.60

UWV is of the opinion that it does not follow from the AP's findings that there is serious culpability negligence. The first four data leaks prompted UWV to make major adjustments to the process and to focus on raising awareness of the risks associated with manual processing. According to Between the fifth and the eighth data breach, UWV deployed to strengthen this organizational measures (such as workshops). According to UWV, this means that in the process of sending group messages in the My Workbook environment has indeed been deployed for security measures to improve.

The AP does not follow this view of the UWV and motivates this as follows. UWV is obliged to provide a apply a security level that is appropriate for the nature and scope of the processing operations carried out by UWV performs. Now that the UWV has not guaranteed an appropriate level of security for years, the AP is of the opinion that UWV has been seriously negligent in not weighing up the risks for citizens, taking appropriate measures

security measures and checking and adjusting these measures. For the organizational
measures that, according to UWV, have been implemented, UWV has not based these measures on
risk assessments and how they considered the possible consequences for those involved. Also has
UWV indicated that it has not checked whether the measures taken after the data leaks
actually implemented and evaluated.

The Wbp, the AVG and the CBP guidelines with regard to the security of the processing of
personal data has expressly described that organizations have a risk-based approach
level of security. The UWV is allowed, partly in view of the sensitive nature and the large size
of the processing is expected to make sure of the standards applicable to it and there
acts on.

In addition, the AP finds it very negligent and negligent that UWV only after nine data breaches in December
In 2018, technical measures were implemented. Namely, blocking the
possibility to add Excel files, among other things, when sending group messages
via the My workbook environment. Citizens who are obliged to provide personal data must
can assume that the UWV, as a government agency, will immediately take the necessary measures to protect their
properly protect personal data.

The fact that the UWV also failed to comply with its own policy rules is also considered culpable by the AP. Despite
that the UWV policy indicates that measures must be taken on the basis of explicit
risk assessments as part of a PDCA cycle, the UWV has not taken sufficient account
with the risks and consequences for job seekers. In addition, UWV will not have a
technical measure introduced while UWV had already decided on October 20, 2016 to implement a
to investigate the possibility of taking technical measures. The UWV also has

59 Parliamentary Papers II 2014/15, 33662, no. 16, p. 1.

60 Acts II 2014/15, 51, item 9, p. 11.

Date

not checked whether the measures that have been taken in response to the data leaks have been actually implemented in the organization. The violation is therefore the result of gross and significant negligence by the UWV.

In the AP's opinion, all of the above shows that the UWV was grossly negligent or considerably negligent has acted negligently, as a result of which there is serious culpable negligence on the part of UWV. Given the circumstances of this case and the criterion of serious culpable negligence under the Wbp, however, the AP sees no reason to reduce or further increase the fine amount.

4.3.3 Proportionality

Finally, the AP assesses on the basis of Article 5:46 of the General Administrative Law Act codified proportionality principle or the application of its policy for determining the amount of the fine, given the circumstances of the specific case, does not lead to a disproportionate outcome.

The AP is of the opinion that, given the seriousness of the violation and the extent to which it can be attributed to UWV accused, (the amount of) the fine is proportionate.61 The organizational measures that, according to UWV, are have been affected, according to the AP, the present infringement of Article 13 of the Wbp and Article 32, first and second paragraph of the GDPR. Failure to weigh up risks to citizens, the lack of having appropriate security measures and not checking and evaluating these measures after all, led to an insufficiently risk-based security level. The violation has In addition, it lasted almost 3 years, during which the privacy of 4,500,000 people was insufficiently guaranteed.

Given all the circumstances of this case, the AP sees no reason to set the amount of the fine on the grounds of the proportionality and the circumstances referred to in the Fining Policy Rules, insofar as applicable the present case, to increase or decrease even further.

4.4 Conclusion

The AP sets the total fine amount at € 450,000.

61 For the justification, see sections 4.3.1 and 4.3.2.

Our reference

[CONFIDENTIAL]

Date

May 31, 2021

5. Operative part

The AP will report to the Employee Insurance Agency for violation of Article 13 of

the Wbp and article 32, first and second paragraph, of the GDPR, an administrative fine in the amount of

€ 450,000 (in words, four hundred and fifty thousand euros).62

Yours faithfully,

Authority for Personal Data,

e.g.

drs. C.E. Mur

Board member

Remedies Clause

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

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

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

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

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

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

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

- Your name and address
- The date of your objection
- The reference mentioned in this letter (case number); you can also get a copy of this decision

attach

 The reason(s) why you disagree with this decision

 Your signature

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

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

Date

May 31, 2021

Our reference

[CONFIDENTIAL]

Attachment 1

1. UWV policy

In the policy documents "Strategic Information Security and Privacy Policy (IB&P)", the UWV has for the period 2016-2020, included: “that management makes decisions based on careful consideration of the risks”.63 It also states the following: “Depending on the outcomes of the analyses, risks are an adequate system of measures neutralized or explicitly accepted by a director. One of these will be centralized registration. UWV continues to ensure continuity, quality and safety. This means that risks are detected early and dealt with in a professional manner”.64

For the most part, UWV has stated in the policy documents “Tactical Policy, Information Security and Privacy (IB&P) Legal Framework", which applied from April 2016 to at least January 2019, included the following: "At the processing and storage of personal data, the required technical and organizational security measures are taken selected and realized in a risk-driven manner, in accordance with UWV Tactical IB&P Policy Section B 'BIR UWV'.” 65

In its policy documents, which applied from April 2016 to at least January 2019, UWV has included the following: “In the processing and storage of personal data, the required technical and organizational security measures selected and realized in a risk-driven manner, in accordance with UWV Tactical IB&P Policy Section B 'BIR UWV'. 66

With regard to checking, evaluating and adjusting measures, UWV states in its

policy document, valid from December 2015 to at least January 2019:67

“4.2. The organizational units: primary actors

IB&P risk management is primarily the responsibility of the organizational units themselves. This should be done within your own line

reported, in accordance with the agreements made in-house. From the central monitoring of the IB&P risks, the organizational units were asked to report on the UWV-wide top IB&P risks.

The organizational units have the following responsibilities:

• Report from the implementation responsibility on the progress of these prioritized measures

and improvement actions (using a format) and any new IB&P risks via the divisional reporting;

• Periodic review of the (BIR) improvement plans containing improvement actions based on the UWV-wide

identified IB&P risks;

63 See file document 38 (Excel file, appendix 6 (file “UWV BZ IBP Strategic Policy v190”, p. 7) and appendix 11 (file "UWV BZ IBP

Strategic Policy v202 (GDPR version)", p 7-8). These appendices are part of file “Document” in answer to question 4 under data breach 1).

64 Ditto.

65 See file document 38 (Excel file, appendix 7 (file “UWV BZ IBP Section A Legal Framework v100.docx”, p. 11) and appendix 10 (file

"UWV BZ IBP Section A Legal Framework v102 (GDPR version)", p. 12). These attachments are part of file “Document” in response to

question 4 under data breach 1).

66 See file document 38 (Excel file, appendix 7 (file “UWV BZ IBP Section A Legal Framework v100.docx”, p. 11) and appendix 10 (file

"UWV BZ IBP Section A Legal Framework v102 (GDPR version)", p. 12). These attachments are part of file “Document” in response to

question 4 under data breach 1).

67 See file document 38 (Excel file, appendix 9 (file “UWV BZ IBP Sectie C Borging BIR Beheersing v200” which is part of file “Document” in answer to question 4 under data breach 1, p. 7-8)).

• Implement measures based on the prioritized UWV-wide IB&P risks and own risk inventory and maintained (via the improvement plans).

4.3. Administrative affairs: coordinating role

The substantive support and monitoring for IB&P is centrally assigned to Administrative Affairs. Administrative Affairs is responsible for the coordination and overall mapping of the IB&P risks. For the obtaining the overall picture, Administrative Affairs carries out the following activities:

• Monitoring the progress and realization of actions and measures in the field of IB&P, such as progress on the improvement plans;

• Periodically conducting a substantive qualitative investigation (Quality Assurance) into the status of the IB&P improvement actions and management of the top IB&P risks at the organizational units;

• Delivery of an IB&P report to the IB&P Coalition and the Board of Directors, periodically or at particularities;

• Coordinating the annual exercise of reassessing UWV-wide risks and (BIR) improvement plans;

• Providing substantive support for the improvement plans and actions to be implemented;

• Keeping an up-to-date overview of the most important UWV-wide IB&P risks”. 68

2. Practice within UWV

2.1 Weighing risks in practice

With regard to the performance of risk analyses, UWV indicates that it: “In general, this is an organization

and also in investigating and preventing data leaks, takes a pragmatic approach. UWV opts for a pragmatic approach

approach with concrete improvements instead of voluminous reports. For example, documents that we refer to as 'risk

analysis'

can be labeled 'research' by the department, which means that either understandably but

the false impression may arise that we are not complete".69

When asked if prior to the decision in 2012 to send group messages by means other than Outlook

sending a risk analysis has been carried out, UWV reports: "There is about sending group messages via the

workbook no risk analysis in itself made".70

When asked how UWV determined in 2012 that sending group messages via the My Workbook

environment is an acceptable risk, which security measures have been considered and how

has been made, UWV replies: "The workbook has a link with SONAR and werk.nl, and the customer must

of his/her DigiD to be able to open and view messages. Moreover, unlike bee

sending via outlook- once sent messages are deleted if a message is sent incorrectly. UWV sees

therefore the workbook as one of the safe channels to exchange data and messages".71

68 See file document 38 (Excel file, appendix 9 (file "UWV BZ IBP Section C Assurance BIR Management v200" which is part

of

file "Document" in answer to question 4 under data breach 1, p. 7-8)).

69 See file document 46 (Reply by UWV, appendix 2 (file "Letter AP information request 29042019", p. 1)).

70 See file document 98 (Answer by UWV, file "Supplementary questions AP2110", page 2, appendix 4 (file "Additional notes

meeting Management Team WERKbedrijf") and appendix 5 (file "28 BV 06 Decision document forbidding the use of group mail

via Outlook")).

71 See file document 98 (Answer by UWV, file "Additional questions AP2110", p. 2).

Date

May 31, 2021

Our reference

[CONFIDENTIAL]

When asked whether the specific data leaks led to a risk analysis

UWV indicates: “UWV and in particular the WERKbedrijf division, following the four leaks in 2016, initiated a risk analysis performed. This risk analysis can be found in the document: 'Voorlegger DMO WERKbedrijf' and her appendices, containing guidelines for employees”.72 This submission of October 2016 states the following included: “To cope with the unrest and disrupt services as little as possible, but at the same time To conduct a thorough analysis of where we run risks in our customer communication, we have taken the following measures for (…)”.73

When asked whether a risk analysis has been carried out after each data breach, UWV stated the following: “During 2016, UWV saw no need to carry out a PIA as such. The Business Security Officer (BSO) of Werkbedrijf has made an evaluation (sic) for the District Managers Consultation regarding the data breaches in August and September 2016. See the proposal - a proposal for decision-making - of the 4th quarter 2016 of the BSO WERKbedrijf with decisions to be made/impact analysis/measures and conclusions and recommendations. In addition in the appendix a guideline Safe Communication at WERKbedrijf. Because there was one leak in 2017, UWV saw no need to to adjust the policy and to carry out a PIA. After the two leaks in 2018, the Board of Directors has removed the Officer Data protection requested to start an investigation”.74

When asked why, after the leak in 2017, UWV did not see the need to carry out a risk analysis stated the following: “UWV has weighed up the balance and, of course, has also given weight to the rights and benefits freedoms of data subjects. In the meantime, with today's knowledge, this consideration may be different”. 75 UWV has upon request, no documents were provided in which the considerations made at the time were recorded.

With regard to data leaks five to eight, UWV reports: “The risk of more leaks was considered low considered and measures from October 2016 seemed to be effective, as we explained earlier in the reply to the information request. At that time, a number of other ICT measures in the systems had a high priority. In retrospect, this was a wrong assessment and technical measures should have been taken sooner”.76

The UWV has not substantiated the basis of the assessment that the risk should be considered low considered.

UWV has stated in relation to the eighth data breach: “The Data Protection Officer (FG) has to

As a result of this data breach, an investigation was carried out into export functionality within the workbook. Then (sic)

performs

the Data Protection Officer (FG) is currently conducting a risk analysis on behalf of the Board of Directors

Sonar”.77

72 See file document 46 (Reply by UWV, appendix 2 (file “Letter AP information request 29042019”, p. 1)).

73 See e.g. file document 38 (Excel file, appendix 27 (file “Microsoft Word 97-2003 document” in response to 11 under data

leak 1

through 4, p. 2)) and file document 102 (Answer by UWV, appendix 2 (file “42DMO-B04. 161017 ES Notitie DMO WB", p.2)).

74 See e.g. file document 38 (Excel file, answer to 11 under data leaks 1 to 4).

75 See file document 81 (Answer by the UWV, appendix 1 (file "Answer to AP August 2019 questions", answer to question

12)).

76 See file documents 65 and 66 (Answer by UWV, p. 2).

77 See e.g. file document 38 (Excel file, answer to 11 under data leak 7).

Date

May 31, 2021

Our reference

[CONFIDENTIAL]

2.2 Measures, control and adjustments in practice

Temporary measures of 28 September 2016

UWV states that it was necessary to implement the measures that applied prior to the fourth data breach

evaluation and that it has decided to take measures.78

UWV reported with regard to the measures after the four data leaks in 2016: “Then are direct

organizational and process measures have been taken to mitigate the risks of recurrence”.79 From the presenter

of October 18, 2016, it appears that on September 28, 2016 - after the fourth data breach - the “DT WERKbedrijf” was among

the

following temporary measures had been decided, which relate to sending messages with

attachments via the My Workbook environment to several job seekers at the same time:80

On September 30, 2016, these temporary measures and the instructions were communicated to the managers

of the WERKbedrijf via the following WORK message:81

78 See e.g. file document 38 (Excel file, answer to question 18 under data breach 1 to 4).

79 See file documents 65 and 66 (Answer by UWV, p. 1).

80 See file documents 65 and 66 (Answer by UWV, appendix, answer to question 2) and file document 102 (Answer by UWV),

appendix 2 (file “42DMO-B04. 161017 ES Note DMO WB", p.1).

81 See file document 98 (Reply by UWV, appendix 2 (file "Werkbericht 30 september 2016", p. 2 and 3)).

UWV states that these temporary measures and the instructions were communicated to on October 4, 2016

all (then employed) employees via a newsletter WERKInUitUitwerp with the following text:82

UWV indicates that the temporary measures mentioned on the previous page will be implemented as soon as possible

entered into force after September 28, 2016. UWV also states this in view of the importance of these measures

and the relevance to the type of risks that mainly play a role in this type of data breach, these temporary measures

would still be in force at this time.83 However, the UWV has not substantiated this with documents.

82 See file document 98 (Reply by UWV, appendix 3 (file “WIU 4 October 2016”)).

83 See file documents 65 and 66 (Answer by UWV, appendix, answer to question 2).

Our reference

[CONFIDENTIAL]

Measures proposed in October 2016

In the submission of October 18, 2016, which was drawn up in preparation for the District Managers meeting

(DMO) on October 20, 2016, the following is stated about the temporary measures mentioned above:84

That is why the DMO was asked in October 2016 to agree to the following measures, ter

replacement of the temporary measures decided on 28 September 2016:85

84 See file document 102 (Reply by UWV, appendix 2 (file “42DMO-B04. 161017 ES Notitie DMO WB", p.2)).

85 See file document 102 (Reply by UWV, appendix 2 (file “42DMO-B04. 161017 ES Notitie DMO WB", p. 2)).

Date

May 31, 2021

Our reference

[CONFIDENTIAL]

During the DMO of October 20, 2016, with regard to the measures proposed above, the

next decided:86

It follows from these minutes that on 20 October 2016 the DMO met only with the (mentioned on page 30)

measures 1 to 6 has been agreed. In addition, it has been decided that measures 7 to 10 -

including an investigation into concrete technical measures - to be taken up in the short term.

UWV indicates that all measures (mentioned on page 30) have been implemented.87 However, UWV has

not (sufficiently) substantiated whether and when the implementation took place. Of the measures

1 to 6, UWV has only demonstrated that the “Guideline for safe communication at WERKbedrijf”.

drawn up.88 As can be seen below, this - undated - Guideline contains basic principles

communicating securely:89

86 See file document 102 (Reply by UWV, appendix 1 (file “42DMO-A04. Decisions and overview of action points 20 Oct.

2016", p. 3

and 4)).

87 See file document 38 (Excel file, answer to question 14 under data leak 1).

88 See file document 38 (Excel file, appendix 33 (file "161020 Appendix A Data Leaks WB", which is part of file "Microsoft Word document" in answer to question 15 under data breach 1)).

89 See file document 38 (Excel file, appendix 33 (file "161020 Appendix A Data Leaks WB", which is part of file "Microsoft Word document" in answer to question 15 under data breach 1)).

It follows from pages 30 and 31 that on 20 October 2016 the DMO decided to launch an investigation into the possibilities of technical measures until further notice. When asked if this research took place, the UWV replied: “No, this investigation has not taken place”.90

UWV reports with regard to the question of how it has been checked whether measures have been proposed after each data breach have actually been introduced: “UWV and WERKbedrijf have not as such checked whether measures have been taken taken as a result of data breaches have actually been introduced. UWV does not have a generic policy in which it checks whether UWV central measures have been implemented by the responsible division(s). Within divisions like

90 See file documents 65 and 66 (Answer by UWV, appendix, p. 1, answer to question 3).

WERKbedrijf that operate throughout the country can, to a certain extent, give regional offices their own interpretation

central policy, for example in awareness campaigns".91 The UWV also reports: "There is no formal protocol procedure within UWV within which it is checked at a central level whether such agreements are made organizational and process measures are implemented. That would be impracticable given the size of the organization and the number of decisions that UWV takes".92 UWV states in response to the actual findings, however, that it would indeed have checked whether the measures taken were in practice have been brought.93 The UWV has not substantiated this assertion with documentation.

To the question of whether and in what way the measures taken by the UWV in response to the first four data leaks had decided have been evaluated, what the results of that evaluation were and whether the desired effect of that was measures had been taken, the UWV reports: "No, given the relatively limited number of leaks from 2017 compared to 2017 in absolute terms.

2016, UWV saw no reason to assume that the mitigating measures did not properly mitigate the risks addressees".94 And: "In 2017, the UWV saw no reason, given the relatively small number of leaks (1), to evaluate measures".95

UWV states the following with regard to the way in which it carries out evaluations: "There is no formal protocol-based evaluation process after each of the seven data breaches. That is not the way UWV at all cases works. The departments involved concluded in good consultation for some time that the measures taken in 2016 measures were sufficient. Unfortunately, this conclusion later turned out to be incorrect."96 UWV states in response to the factual findings, however, that evaluations have been carried out with regard to the measures taken.97 These UWV has not substantiated this claim.

Fifth data breach

UWV has indicated that after the fifth data breach, further efforts have been made to raise awareness in the sending messages via the My Workbook environment.98 In that context, after the data breach on 20 July 2017, UWV sent the following WORK message to managers of the WERKbedrijf:99

91 See file document 38 (Excel file, answer to question 16 under data breach 1 to 7).

92 See file documents 65 and 66 (Answer by UWV, appendix, p. 2, answer to question 4).

93 See file documents 109 and 116 (UWV response to factual findings, p. 3).

94 See e.g. file document 38 (Excel file, answer to question 18 under data leak 6).

95 See e.g. file document 38 (Excel file, answer to question 18 under data breach 1 to 4).

96 See file documents 65 and 66 (Answer by UWV, appendix, p. 2, answer to question 5).

97 See file documents 109 and 116 (UWV response to factual findings, p. 3).

98 See e.g. file document 38 (Excel file, answer to question 13 under data breach 5).

99 See file document 38 (Excel file, appendix 31 (file "Microsoft Word document" in answer to question 14 under data leak 5)).

UWV also states with regard to this data leak: "As a result of this leak, UWV/WERKbedrijf has issued the 'Secure communication'" and UWV has added the “Guideline for safe communication at WERKbedrijf” to the answers to questions about the fifth data breach have been added.100 Based on the information on page 31, it seems however, to follow that this guideline was already drawn up after the fourth data breach. And as mentioned before, UWV has not provided any evidence that the measure has actually been introduced or checked.

UWV further states with regard to the fifth data breach in 2017: “Important for the decision to, at the time, after this leak, not taking any extra technical measures was mainly a full release agenda, in combination with a far-reaching change assignment for WERKbedrijf”.101 The UWV has not supplied any documents containing this decision contained.

With regard to the question of how the aforementioned measures have been checked, the UWV has also checked have actually been carried out answered that UWV and WERKbedrijf have not as such checked whether measures taken as a result of data breaches are effective entered.102

100 See e.g. file document 38 (Excel file, answer to question 18 under data leak 5).

101 See file document 81 (Answer by UWV, appendix 1 (file "Answers to AP August 2019 questions"), answer to question 12).

102 See file document 38 (Excel file, answer to question 16 under data leaks 1 to 7).

To the question of whether and in what way the measures that UWV had decided to take after the fifth data breach evaluated, what the results of that evaluation were and whether the desired effect of those measures was reached, UWV reports: "No, no evaluation has taken place after this leak because it was considered an incident for which the mitigating measures seemed effective at the time".103

UWV states the following with regard to the way in which it evaluates measures: “There is none formally documented evaluation process after each of the seven data breaches. That is not the way UWV works in all cases. The departments involved concluded in good consultation for some time that the measures taken in 2016 measures were sufficient. Unfortunately, this conclusion later turned out to be incorrect.”104 UWV states in response to the factual findings, however, that evaluations have been carried out with regard to measures taken.105 These The assertion that an evaluation has taken place is not substantiated with documentation from which the evaluation is based actually appears.

Sixth through ninth data breaches (2018)

UWV has indicated that there are no measures in response to the sixth data breach on 26 March 2018 affected.106 According to UWV, after the seventh data breach on March 28, 2018 and the eighth data breach on August 3, 2018, decided on the following measures:107

"-Workshop Prevention Data Leaks

This is a workshop aimed at increasing awareness of working with personal data and the conducting risk analyzes together. The workshop was handed over to representatives from all over the world via the 'train the

trainer'

labor market regions, who then rolled out the training across the branches.

- Common toolkit page on DWU

Partly as a result of the introduction of GDPR, the toolkit page of the IB&P has been further expanded and there is a lot of material

offered. This is partly in support of the workshop mentioned above.

- Step-by-step plan Safe sharing of personal data

In light of the entry into force of the GDPR, the old 'Secure Digital Communication' guideline has been replaced by the guideline 'Step-by-step plan Safe sharing of personal data'

- Attention from management

The Information Security & Privacy & Security consultation is held annually with the regional management. Also there is currently a UWV-wide IB&P training for managers, including a breakout session 'data leaks and role management therein'

- SLIM rollout

During the roll-out of SLIM working, a lot of attention is paid to safe working and the prevention of data leaks. This both during MT sessions, as well as during branch-wide kick-offs.

Technical measure:

103 See e.g. file document 38 (Excel file, answer to question 18 under data leak 5).

104 See file documents 65 and 66 (Answer by UWV, appendix, p. 2, answer to question 5).

105 See file documents 109 and 116 (UWV response to factual findings, p. 3).

106 See file document 81 (Answer by UWV, appendix 3 (file "Question 7 appendix 2")).

107 See e.g. file document 38 (Excel file, answer to question 13 under data leaks 6 and 7).

Date

May 31, 2021

Our reference

[CONFIDENTIAL]

Attachments blocker

WERKbedrijf has made it impossible through an early release in the weekend of December 15/16, 2019 (sic)

made to attach Excel files in the Workbook to messages even longer."

With the exception of the measure with regard to the "Step-by-step plan for the safe sharing of personal data" and

UWV has not provided any documents or further substantiation based on the technical measure

of which it can be determined how the above-mentioned measures are safeguarded in documentation.

Furthermore, it has not become clear when the above measures were implemented.

UWV has provided a version of the "Step-by-step plan for the safe sharing of personal data". That roadmap is

dated April 26, 2018 and therefore drawn up after the seventh data breach. UWV explains: "In the light

of the entry into force of the GDPR, the old guideline 'Secure Digital Communication' has been replaced by the guideline

'Step-by-step plan for Safe Sharing of Personal Data'.108 This step-by-step plan is as follows:

108 See file document 38 (Excel file, answer to question 13 under data leaks 6 and 7).

Date

May 31, 2021

Our reference

[CONFIDENTIAL]

Date

May 31, 2021

Our reference

[CONFIDENTIAL]

The step-by-step plan will be available on 1 May 2018 via the newsletter to employees of WERKbedrijf

communicated:109

When asked whether there are technical measures between the first and the eighth data breach on August 3, 2018

implemented, UWV replied: “UWV did not implement any technical measure during that period,

but implemented several organizational and process-related measures. However, we believe that this fact

must be viewed in the light of the risk assessment made by the UWV at the time and the arrears outlined earlier

the area of IB&P measures as a result of targets, which is described in the letter”.110

After the eighth data breach, UWV analyzed on August 20, 2018 how the data breach could have happened

take place and how this specific data breach was handled towards those involved. This analysis has been described

in a document containing the following recommendations:111

109 See file documents 109 and 116 (UWV response to factual findings, appendix “WORK in progress”, point 07).

110See file documents 65 and 66 (Answer by UWV, appendix, p. 1, answer to question 1).

111 See file document 38 (Excel file, appendix 42 (file “Microsoft Word document" in answer to question 18 under data leak 7),

p. 3).

Date

May 31, 2021

Our reference

[CONFIDENTIAL]

Furthermore, UWV has stated about the analysis mentioned above: “First of all, WERKbedrijf

2018 based on an analysis of what went wrong in Alkmaar (…) - not following the organizational and

process-based security rules- again sent an instruction to employees for handling bulk messages via

the Workbook to prevent this type of leak. More research in the sense of a comprehensive report is not an option here

basis because the cause was clear. (…) Based on this analysis, UWV has also decided to take technical measures

take - where it was previously established that organizational and process-related security measures were sufficient - i.e. An

to build a blockade in the Workbook so that, among other things, no Excel files can be sent with it, which means that mid

December happened”.112

On September 3, 2018, one month after the eighth data breach and two days prior to the ninth

data breach, the QRC group messages has been expanded with a boxed passage with instructions to prevent data breaches

to avoid:113

112 See file document 46 (Reply by UWV, appendix 2 (file “Letter AP information request 29042019”), p. 1).

113 See file document 91 (Reply by UWV, appendix 4 (file "Sending QRC Sonar Group message to the Workbook 22072013", p. 1)).

At the first point in the passage mentioned above from QRC group messages of September 3, 2018 states that the export lists for sending group messages must first be created by the employees are cleaned by deleting data from the file. This leaves only the row ID about. Furthermore, this version of the QRC group messages states that the 4-eyes principle must be used become. In earlier versions of the provided QRC group messages, these instructions were about the clean and not include the row ID and the 4 eyes principle.

On September 4, 2018, the AP had a telephone consultation with the DPO of UWV. In it is below others considered whether technical measures had been introduced in the meantime. In that conversation the DPO has indicated that, as far as he is aware, no technical measures were introduced. He also indicated that the four-eyes principle had been introduced. He found that the method is inherently insecure as data is extracted from a system and placed in a office application are further processed. He was of the opinion that employees of UWV with a system that has insufficient safeguards.114

Following the eighth data breach, the DPO of UWV has, at the request of the Executive Board of UWV conducted an investigation and described this in the "FG report of findings: Data breach Alkmaar" of 30 November 2018.115 On 22 January 2019, the DPO presented the results of that investigation to the Council of Board and management of Werkbedrijf presented.116 This presentation included, among other things:

114 See file document 22 (Telephone note FG UWV).

115 See file document 81, appendix 5 (file "Question 16_Concept FG report") and file documents 109 and 116 (UWV response to actual findings, p. 3).

116 See file item 38 (Excel file, answer to question 11 under data breach 7) and file item 51 (file “Results FG investigation Work mode v010”, p. 7 and 9).

Date

May 31, 2021

Our reference

[CONFIDENTIAL]

“Measure to disable upload of Excel files to workbook works for this particular vulnerability.

(…)

Placing plasters: Process agreements are not 'hardly' enforced” (…)

“Policy does not reach the workplace:

 Understanding process agreements

 Awareness does not reach all employees”

Ultimately, UWV introduced a technical measure in mid-December 2018, namely blocking of the possibility to add, among other things, Excel files when sending group messages via the My workbook environment.117

With regard to the question of how has it been checked whether measures have actually been taken? entered replied that UWV and WERKbedrijf have not checked whether measures have been taken as such have been taken as a result of data breaches have actually been introduced.118

When asked whether UWV had commissioned external parties to investigate the data leaks, UWV replies with regard to the first eight data breaches: “UWV did not see any added value at that time value in having an external investigation carried out because, given the measures taken, the risk is mitigated

layman”.119 UWV did state with regard to the eighth data breach: “UWV Internal investigation by Administrative Affairs commissioned by FG whereby external expertise has been obtained from a consultant”.120

UWV states the following with regard to the way in which it carries out evaluations: “There is no formal protocol-based evaluation process after each of the seven data breaches. That is not the way UWV at all cases works. The departments involved concluded in good consultation for some time that the measures taken in 2016 measures were sufficient. Unfortunately, this conclusion later turned out to be incorrect.”121 UWV states in response to the factual

findings, however, that evaluations have been carried out with regard to measures taken.122 These

The assertion that an evaluation has taken place is not substantiated with documentation from which the evaluation is based actually shows.

117 See file document 38 (Answer by UWV, letter), file document 38 (Excel file, answer to question 13 under data leaks 6 and 7),

file documents 65 and 66 (Answer by UWV, p. 2 and appendix, p. 1, answer to question 2) and file document 81 (Answer by UWV, appendix 1 (file "Answer to AP August 2019 questions", answer to question 17)).

118 See e.g. file document 38 (Excel file, answer to question 17 under data breach 1 to 7).

119 See file document 38 (Excel file, answer to question 12 under data breach 1 to 6).

120 See file document 38 (Excel file, answer to question 12 under data leak 7).

121See file documents 65 and 66 (Answer by UWV, appendix, p. 2, answer to question 5).

122 See file documents 109 and 116 (UWV response to factual findings, p. 3).