Confidential/Registered

UWV

Board of Directors

attn. M.R.P.M. Camps

PO Box 58285

1040 HG

AMSTERDAM

Date

May 31, 2021

Our reference

[CONFIDENTIAL]

Contact

[CONFIDENTIAL]

Topic

Decision to impose a fine

Authority for Personal Data

PO Box 93374, 2509 AJ The Hague

Bezuidenhoutseweg 30, 2594 AV The Hague

T 070 8888 500 - F 070 8888 501

authority data.nl

Dear Mr Camps,

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

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

insufficiently guaranteed and guaranteed a risk-adjusted level of security 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, first and second paragraph,

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 DPA assesses whether personal data is being processed, the

processing responsibility and the violation. In chapter 4 the (height of the) administrative

fine and Chapter 5 contains the operative part and the remedies clause.

1 Introduction

1.1 Relevant government agency

This Decree relates to the Employee Insurance Agency Implementing Institute (hereinafter: UWV). Ever since

In August 2016, nine data breaches of a similar nature took place at UWV. The

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

An incorrect (Excel) file with a multitude of sensitive and special files was

personal data of a varying number of job seekers that can be included 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 period of two years nine similar data breaches had occurred despite that

UWV had indicated that it had taken measures, it was suspected that UWV did not

technical and organizational measures (as required by law) to ensure an appropriate

security level to prevent new similar data breaches.

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

and with 2018.

1.2 Process

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

data protection officer (hereinafter: DPO) of UWV. Supervisors of the AP subsequently

repeatedly requested information 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. By letter dated 11 March 2021, the AP

sent an intention to enforce 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 Tasks UWV and communication with job seekers

UWV was established on the basis of Article 2, first paragraph, 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 deals with job placement and reintegration. This does

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

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

Persons who wish to apply for benefits under the Unemployment Insurance Act must register with the UWV

register as a job seeker.3

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

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

benefits, they can make changes, tasks and job application activities via My Workbook

pass on and exchange messages with attachments with UWV.5

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

must send. These UWV messages appear in the My Work folder environment of job seekers

justly.

2.2 Source system with stored job seekers data: Sonar

Sonar is the main source system that the WERKbedrijf and municipalities use to help job seekers

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

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

job seekers, the sick and the disabled.7

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

person, all data fields are filled in.8 The data in Sonar concerns, among other things, name and address,

education (level), nationality, citizen service number, data on physical limitations, psychological and physical

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

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

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

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

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

5 See, among other things, file document 120 (pages website werk.nl 'Manual: Using work folder').

6 See, among other things, file document 6 (Presentation Program Council on UWV applications, p. 2, 3, 6 and 11).

7 See file 38 (Excel file, answer to question 6 in the case of data breach 1) and file 98 (Reply by UWV, file

“Additional Questions AP2110”, p. 1).

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

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

Date

May 31, 2021

Our reference

[CONFIDENTIAL]

This data may concern the mood or perception of the job seeker, who is himself an online

completed questionnaire.9

Sonar has about 15,000 users. Half of the total number of accounts belong to the 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, the management of the WERKbedrijf, after data leaks via e-mail, informed the

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

several jobseekers at the same time.11 It was also then decided to adopt this decision together with the Quick Reference Card “Send Sonar Group Mail to the Workbook” forcing to the attention of the executive

employees of UWV.12 A Quick Reference Card is issued 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

job seekers.13 First of all, a UWV employee selects a certain group

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

from UWV this set of data from specific people 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 protected,

because, according to UWV, this would complicate implementation.14 This file is then used as the basis

to determine the recipients of the group message.15 The group message will be sent by the

UWV then visits the recipients in the My Work Folder environment. This dissemination process

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

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

9 See file 38 (Excel file, answer to question 2 for data breaches 1 to 7) and file 81 (Reply by UWV, appendix 1 (file "Answer questions AP August 2019", answer to question 3) and appendix 2 (file "Question 3 - appendix")).

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

11 See, among other things, file 98 (Reply by UWV, file "Additional questions AP2110", p. 3 and appendix 6 (file "29-12 action points list DT", p. 3 under point 4)).

12 See file document 98 (Reply by UWV, file "Additional questions AP2110", p. 2 and appendix 4 (file "28 BV 06 Semitrailer prohibit Outlook group messages 0406212") and attachment 5 (file "28 BV 06 Decision document prohibit the use of group mail via Outlook")).

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

14 See file 38 (Excel file, under “Short description” with regard to all data breaches) and file 81 (Reply by UWV, appendix 1 (file "Answer questions AP August 2019", answer question 11)).

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

16 See file 38 (Excel file, appendix 29 (file "Microsoft Word 97-1003 document" with explanation to answer to question 13 with data breach 6 and 7)), file document 91 (Reply by UWV, appendices 1 to 4).

Date

May 31, 2021

Our reference

[CONFIDENTIAL]

According to UWV, there is a limitation on the number of people when sending a group message to whom the message can be sent.17 Since mid-2013 to the present, this number has been limited to 100 every other month prevent technical problems in Sonar, which improves its operation and stability and message traffic runs more smoothly.18 All used versions of the QRC group messages state that if

a UWV employee still wants to approach more than 100 people via the My Work Folder environment, this can be requested from the Functional Management. Functional Management can limit the maximum very temporarily increase to a larger number of people.19 The QRC group messages also state that attachments can be added are sent along with group messages via Sonar, but it is preferable not to do so.20

In the period from January 2016 to September 2018, according to the 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

Since the beginning of 2016, a total of nine data breaches have taken place related to the personal environment of job seekers: Mijn Werkmap.22 UWV has reported eight of these data breaches 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 removed when the group message is created Sonar added. As a result, this file came with the export (instead of a message that had sent such as a vacancy text) in the My Workbook environment of job seekers justly. As a result, the non-secured and accessible file with the individual data about all message recipients 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 (Reply by UWV, appendix 1 (file "Answer questions AP August 2019", answer question 11)).

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

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

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

21 See file document 86 (Reply by UWV, appendix 1 (file “numbers_posts_ap”)) and file document 91 (Reply by UWV, appendix 5 (file "numbers_posts_ap")).

22 See, among other things, file documents 8 to 12 and 15 to 21 (data breach (follow-up) notifications to the AP) and file 38 (Excel file, reply to question 6 regarding all data breaches).

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

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

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

25 Source of this data: see file 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 of

involved

of which the

data is

leaked

Number of

stakeholders who

the message

have opened

Date

May 31, 2021

Our reference

[CONFIDENTIAL]

1

2

3

4

22-8-2016

195

14-9-2016

151

15-9-2016

135

22-9-2016

11062

14

20

26

26

5

21-2-2017

189

10

6

3/26/2018

10

7

28-3-2018

90

7

12

Surname, Citizen Service Number (BSN), last occupation,

education level and row ID

Surname, place of residence, date of birth, social security number,

first WW day, date on which WW ends and

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

not reachable by SMS or not being digitally skilled

Social Security Number

Surname, zip code, city, e-mail address,

BSN, age, gender, profession (sector),

education (level), first unemployment benefit day and date

on which WW ends, or status of CV active or

has expired, number of days WW on which

job seeker has right, row ID

BSN, initials, surname, gender, e-mail

email address, age, WERKbedrijf location, first

WW day, total score on the online questionnaire and

a brief description of barriers to

with regard to finding work (such as psychological

or physical work ability), including for 73

health data involved. This one

health data does not concern a disease or

medical reports, but, for example, whether

someone is too sick to work. From the first WW

day it can be deduced that all 189 people involved

receive unemployment benefits (not the amount

of them).

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

and social security number

Last name, zip code,

place of residence, professional sector and BSN

6/41

Date

May 31, 2021

Our reference

[CONFIDENTIAL]

8

03/08/2018

2503

70

Surname, gender, date of birth, social security 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 day of unemployment, maximum last day of unemployment

benefit, age group based on first unemployment benefits

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

ID.

9

5-9-2018

996

9

2.5 Policy within UWV

Within the UWV, from at least 2016, a policy had been drawn up to reduce risks in the processing of
detect and deal with personal data early on the basis of a careful risk assessment,
where risks are neutralized or explicitly accepted by a director. Also,
UWV to register the (outcomes of) risk assessments based on the policy.26
Within the UWV, at least from 2016 to 2020, a policy was drawn up to ensure that technical and
implement and implement organizational security measures in a risk-based manner
check, evaluate and adapt.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
personal data when sending group messages.28 How and what risks UWV
has weighed up precisely, partly in response to the data breaches that have occurred, to determine whether
personal data when sending group messages via the My Workbook environment is sufficient then
UWV has not stated that there is insufficient security.29
In its answers, UWV does not appear to provide an unambiguous and even sometimes contradictory picture about the
(periodically) performing risk analyzes with regard to the security of personal data at the
sending group messages via the My Workbook environment. UWV has in any case stated that it

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

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

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

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

Date

May 31, 2021

Our reference

[CONFIDENTIAL]

did not perform a risk analysis prior to the 2012 decision to go group messaging
send via the My Workbook environment. UWV has stated on a number of occasions 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 Work Folder environment has carried out risk assessments. From the
answers from the UWV and the documents provided, however, it has not become clear what these risk assessments are like
made and which risks were considered at any time during that period. UWV also has the
risks not regularly weighed.30

2.6.2 Measures, checks and adjustments in practice

UWV stated in the data breach notifications 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 indicated that UWV was investigating whether it was possible to place "such"
files" in the My Work Folder environment.32 UWV stated in the data breach notifications to the AP
of the third and fourth data breach at the end of September 2016 that the employee who made the mistake
this was addressed by management and that awareness was being looked into.33

After the first four data breaches in 2016, UWV decided to take organizational measures.
On 28 September 2016, UWV first decided to take temporary organizational measures.34 And although
The UWV has stated that these temporary measures are still in effect today, as a result of a decision of the
District managers consultation (DMO) of UWV that the temporary measures to be taken on September 28, 2016
was decided, were replaced in October 2016 by other organizational measures. Furthermore, the
AP established that UWV has drawn up the "Guideline for safe communication at WERKbedrijf" and that it is
intention to investigate the possibilities of taking technical measures is not

UWV has been carried out. In addition, the AP concluded that the in force after October 20, 2016 organizational measure(s) prior to the fifth data breach has not been checked nor evaluated by UWV.35

UWV subsequently decided after the fifth data breach (21 February 2017) to further measures regarding the sending of group messages via the My Workbook environment, namely by raising awareness. UWV did this through workshops and a few visits to districts. UWV then decided not to take any technical measures. Incidentally, the after 20 October 2016 organizational measure(s) in effect with regard to 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 The statement of UWV that these measures did check and evaluated, UWV has not substantiated it 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 breach notifications).

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

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

34 See appendix 1, pages 28 and 29 for the exact measures taken by the UWV.

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

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

After the seventh data breach (March 28, 2018), UWV decided to take several organizational measures. However, UWV and the WERKbedrijf have not checked as such whether these measures are actually have been introduced.37 Apart from two measures38, UWV also has no documents or a further

substantiation provided on the basis of which it can be established 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 to add Excel files when sending group messages via the My Workbook environment to prevent data leaks to prevent. This technical measure was implemented by UWV in December 2018, so far after the ninth data breach implemented.

The above facts relate to the period from 2012 to 2018. This decision and the investigation of the AP only cover this period. In its view, UWV still has the following declared for the period after 2018.

UWV has stated that in the process for sending group messages in the My Work Folder environment in addition to the technical measure, which has the specific risk of sending Excel lists removed, an active effort has also been made to raise awareness among (new) employees in the implementation have frequent (digital) contact with job seekers for the performance of their tasks. In addition Within WERKbedrijf, the process descriptions and Quick Reference Cards (QRCs) are now published annually evaluated and adjusted if necessary.

Furthermore, at the end of 2018, the DPO carried out an investigation on behalf of the Board of Directors of UWV drawn up in response to the eighth data breach and a report of findings. Specific to the mitigating the risks when sending group messages in the My Workbook environment, it states DPO investigation that the technical measure that uploads Excel files to the My Workbook environment impossible is an effective measure to prevent this type of data breach.

Partly as a result of the DPO investigation, UWV WERKbedrijf has further instructed KPMG: given to conduct a broader investigation of the source system SONAR. This is to determine where the vulnerabilities and risks are located on a technical, process and organizational level, 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

privacy advisory report has largely been made public by UWV.39

As a result of the advisory reports, the large-scale improvement project SONAR IB&P was started in 2020,

that aims to address the findings of the study and SONAR .'s IB&P risk level

strongly reduced (act->plan->do phases). In that context, UWV will take an extra technical measure

37 See appendix 1 on pages 35 to 41 for the exact measures and statements of the UWV.

38 The Step-by-step plan for Safe Sharing of Personal Data, which UWV communicated to employees on 1 May 2018. Also had

UWV expanded 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-research report-sonar-privacy.pdf.

implement. The export functionality from SONAR for employees in the implementation, except for some

authorized employees, will be closed.

According to the 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

WERKbedrijf the growth in fleshing out the PDCA cycle – and thus guaranteeing that there are

appropriate technical and organizational measures have been taken and will be continued.

3. Legal Review

3.1 Processing of personal data

As of 25 May 2018, the General Data Protection Regulation (GDPR) applies.40 In view of the

facts in this investigation took place between 2012 and 2018, the AP will comply with both the Protection Act

personal data (Wbp) as the AVG.

The term personal data is defined in Article 1, under a, of the Wbp and Article 4, part 1, of the GDPR. In Article 16 of the Wbp, personal data about health are regarded as special identified as personal data. The GDPR also considers 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, citizen service number (BSN) and other data. With this data the registered in Sonar can natural persons, including job seekers, are identified directly or indirectly. Sonar contains i.e. personal data within the meaning of Article 1(a) of the Wbp and Article 4(1) of the GDPR.

Sonar also includes data on physical limitations and the psychological and physical people's work ability. Sonar also states whether people feel too ill to work. on pursuant to Article 16 of the Wbp and Article 4(15) of the GDPR, these are data about the health.

It follows from the above that UWV when sending group messages via the My Work Folder environment personal data, including the citizen service number (BSN) and health data, processed within the meaning of the Wbp and the GDPR.

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

Date

May 31, 2021

Our reference

[CONFIDENTIAL]

3.2 Controller

The term (controller) is defined in Article 1, under d, of the Wbp and Article 4, section 7, of the GDPR. In the case of independent administrative bodies at state level, the body charged with the tasks and exercise of powers for which the data is processed, as a controller

are to be noted.

As stated in section 2.1, UWV was established on the basis of a law, namely the SUWI. UWV is a independent administrative body of the national government with its own legal personality. As above In the case of independent administrative bodies at state level, the body charged with the duties and performance is stated of powers for which the data is processed, as responsible. UWV has both legal and de facto control over the processing of personal data that are collected in the context of sending group messages via the workbook.

On the basis of the above, the AP designates the UWV as a controller or controller as referred to in Article 1(d) of the Wbp and Article 4(7) of the GDPR 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 process of data processing. The term "appropriate" implies that the security in conforms to the state of the art. This is primarily a question from professional ethics of persons charged with information security. The standards of this ethics are set forth in this provision of a legal final element, in the sense that it imposes a legal obligation for the responsible 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 have a more sensitive nature, or the context in which they are used a greater threat to the personal 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 drafted considers: other 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 individuals, public authorities, undertakings or other bodies carrying out the processing operations are imposed, obligations that are in particular

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

authority and the circumstances in which the processing may be carried out (…)".41

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

rights and freedoms of data subjects in relation to the processing of personal data both in 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 and on the free movement of such data, recital 25. Underlining the AP.

requires appropriate technical measures in the execution of the processing, in particular to ensure security

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

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

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 that

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 order to implement Article 13 of the Wbp, the Dutch DPA issued security guidelines in 2013

of the processing of personal data (hereinafter: Dutch DPA guidelines).44 When drawing up the

CBP guidelines have been sought to link up with ISO27001. The guidelines state as necessary

preconditions to ensure a continuous appropriate level of security for the processing of

obtain and guarantee personal data as prescribed by law: "take measures based on

risk analysis, applying security standards and embedding it in a plan-do-check-act cycle".

The Dutch DPA guidelines state about this PDCA cycle: "After establishing the reliability requirements, the

responsible measures to ensure that the reliability requirements are met. Thereafter

the controller checks whether the measures have actually been taken and are having the desired effect. The total reliability requirements, measures and controls are regularly evaluated and adjusted where necessary, so that a permanently 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, whereby he identifies threats that could lead to a security incident, the consequences that the security incident and the likelihood that these consequences will occur. When inventorying and assessing the risks, the consequences that data subjects may experience from unlawful processing of their personal data. These consequences can, depending on the nature of the the processing and of the personal data processed, including in the form of stigmatization or exclusion, harm to health or exposure to (identity) fraud.46

Article 32 of the GDPR sets out the requirements for the security of the processing of personal data Hospitalized. When determining appropriate measures, the risk should be taken into account 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 to prevent the

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

43 See, inter alia, case Z2003-0145, p. 3.

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

45 See Dutch DPA 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.

Date

May 31, 2021

Our reference

processing infringes this Regulation, the controller or processor shall

processing inherent risks 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 compared to the risks and the nature of the

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

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

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

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

Finally, in 2007 the Government Information Security Regulations Decree (hereinafter: VIR) came into effect

48 In the 2014 Administrative Declaration on Information Security, the UWV declares that it will follow the VIR

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

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

ISO17799:2005 has since been incorporated into 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 (ever-changing) threats to information.52

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

explanation to the VIR, the following is included about Article 4 of the VIR: "It was a conscious decision to introduce Article 4

formulate terms of the Planning and Control cycle, in accordance with regular business operations. (…) Information security

itself

takes place via the Deming quality circle (PDCA cycle)".53 The article-by-article explanation of the VIR states

in addition with regard to Article 4: "For the effectuation of information security, we work via the Plan Do

Check Act cycle (...). After determining what is necessary (reliability requirements), measures are taken and

checked whether those measures have the desired effect (control). This check can lead directly to

adjustment of the measures. The total of requirements, measures and checks may also need revision (evaluation). It

properly completing this quality circle ensures the adequate security level at all times".54

3.3.2 Assessment

It follows from both Article 13 of the Wbp and Article 32(1) and (2) of the GDPR that the

controller must take appropriate technical and organizational measures to

risk-adapted security level of the processing of personal data

guarantee/guarantee. These provisions are intended to safeguard the same (legal) interests and there is no

(substantial) material change in the regulations on this point.

To ensure a risk-adjusted level of security for the processing of personal data

guarantee/guarantee, a controller should thus analyze risks, make 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, among others, 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.

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

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

namely by embedding 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

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

is based on ISO27001 and prescribes a PDCA cycle. This general

accepted security standard, the AP also takes into account in this case. The AP works the

different steps of the PDCA cycle further below.

Weighing the risks for people before determining measures

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

personal data is a consideration of the risks of that processing. Based on this, it is determined

what measures are necessary to counter these risks.

It follows from the Wbp and the AVG and their explanation that when considering the data security risks

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

unauthorized disclosure of or access to processed data. When inventory

and assessing the risks, the consequences that persons may experience from a

unlawful processing of personal data. The more sensitive the data is, the more

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

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

When sending group messages via the My Work Folder environment, as stated in paragraph 2.4,

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

access to processed personal data of job seekers. The UWV is therefore expected to

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

assesses that could lead to a security incident. Within the UWV, there was in any case from 2016

policy to detect and address risks in the processing of personal data early on

based on careful risk assessment. The VIR also obliges UWV to carry out an explicit risk assessment in

determining appropriate security measures.

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

personal data of a very sensitive nature, including data about the health of persons

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

persons. Jobseekers, the sick and incapacitated for work who are legally obliged to register with

UWV and therefore have to provide their personal data, must be able to rely on 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 can not sufficiently secure the processing of these

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

makes it much easier in practice to link different files, there is for individuals

whose data resides in Sonar poses an additional risk 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 in their response to the

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

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 Work Folder environment no risk analysis has been performed. Subsequently, UWV stated

that from 2016 up to and including the last data breach in 2018, in the context of the security of

personal data when sending group messages via the My Workbook environment

carried out risk assessments. However, it is not clear from the answers of the UWV and the documents supplied

it has become apparent how UWV has made these risk assessments and which risks are involved at any time during that

period

period have been considered and how this has been considered with the possible consequences for job seekers. In front of

to the extent that UWV is of the opinion that the proposed measures of October 201655 are a risk assessment

contains, the AP notes that no consideration of risks in the sense of the (interpretation of the) law is

to take. It contains only a proposal for measures without further substantiation. It also appears from
This document does not state that risks to persons have been considered when proposing measures. Stronger
still, UWV only talks about risks that UWV itself runs in its customer communication. Right at a
organization such as UWV, which processes so many special and sensitive personal data of so many people,
and the consequences for them when sending group messages through the My Workbook environment
can be far-reaching, it is not or insufficiently taking into account the risks for job seekers
extra careless when determining security measures.
On the basis of the above, the AP concludes that UWV with regard to taking
security measures in the context of sending group messages via the My Work Folder
environment the risks for job seekers, which, given the sensitivity of the data processed by UWV
can be radical, at least not/insufficiently mapped out in the period from 2012 to 2018
has brought. As a result, UWV does not have a sufficiently risk-adjusted security level
guaranteed and guaranteed.
Taking technical and organizational measures
After mapping and weighing the risks for individuals of the processing of personal data
the determined measures must then be implemented and carried out. Both article
13 of the Wbp as well as Article 32(1) of the GDPR oblige the controller to
taking technical and organizational measures to ensure the security of the processing of
to safeguard personal data.
Section 2.6 shows that until December 2018 UWV only has organizational measures
implemented in the context of sending group messages via the My Workbook environment to
to ensure the security of the processing of personal data. An example of a
55 See appendix 1 page 30.

Date
May 31, 2021

organizational measure, the message where employees are summoned is preferably no
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 continued, as UWV itself states,
to prevent technical problems in Sonar that improve its operation and stability and
message traffic runs more smoothly. This does not serve to protect the security of the processing of
to safeguard personal data. This limitation only applies to the number of recipients of a message,
but does not limit the number of job seekers whose personal data can be collected by UVW
sent. In addition, the limitation to 100 recipients could be circumvented by a request to do so
to do with Functional Management. In five of the nine data breaches, the same group message has been sent to more than
100 job seekers sent simultaneously via the My Work Folder environment.
UWV decided on 20 October 2016 (after the fourth data breach) to conduct an investigation in the short term
start looking at 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 UWV subsequently decided to take
a technical measure, namely blocking the possibility to add, among other things:
Excel files when sending group messages through the My Workbook environment. However, it turns out that
UWV only in December 2018 (far after the ninth data breach on September 5, 2018 and far after the 2016
announced investigation into the introduction of technical measures) has proceeded every three
actually implement the decision taken months earlier. Taking this technical
measure was therefore possible.
The data leaks apparently did not constitute an urgent reason for UWV to carry out the investigation suggested in 2016.
to be able to implement technical measures as soon as possible. By not (also)
implementing a technical measure, UWV has insufficiently adjusted a risk
security level guaranteed and therefore 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 serve both on the basis of 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, applied or implemented correctly 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 for the risk
security level or whether additional measures are required.

Within the UWV, from at least 2016 to 2020, a policy will apply to prevent measures taken
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 a certain extent
can give their own interpretation to central policy. The Employee Insurance Agency (UWV) also reports that there is no
is a formal protocol procedure within UWV, within which measures are taken at a central level

checked whether such agreed organizational and process measures are
carried out, because that would be impracticable given the size of the organization and the amount of
decisions taken by UWV.

The UWV also states that it has not checked whether measures that had been decided in response to
of data breaches have actually been introduced. In addition, the UWV has entered into force after 20 October 2016
being organizational measure(s) prior to the fifth (2017) and sixth (2018) data breach not
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. UWV has also not evaluated these organizational measures.
As concluded earlier, the consequences for job seekers when sending insufficiently secured
of group messages through the workbook providing. Especially at an organization like UWV, which has so many sensitive
and special personal data of so many people, it is necessary to check whether
measures have actually been (correctly) implemented and to evaluate them and adjust them where necessary
to suit. Job seekers and others who are legally obliged to register with UWV and for that purpose
must provide their personal data, must be able to rely on UWV measures
checks, evaluates and adjusts if necessary.
Based on the above, the AP concludes that UWV has implemented the security measures taken in the
framework of sending group messages via the My Work Folder environment does not / is insufficient
checked and evaluated, as a result of which UWV does not have a sufficient security level tailored to risk
has guaranteed and guaranteed.

3.4 Opinion UWV and response from AP

In this section, the AP briefly summarizes the UWV's view, along with the AP's response.
The UWV first of all notes that it regrets that insufficient substance has been given to the
different phases of the PDCA cycle. UWV is very keen on the findings of the AP and puts it firmly on it
to improve this process.

3.4.1 View of factual findings

UWV is of the opinion that the analysis of the eighth data breach shows that the eighth data breach and the
measures have been both analyzed and evaluated by UWV, whereby measures are also proposed.
The AP notes in this regard 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 has evaluated itself. The evaluation of a
individual data breach is insufficient implementation of a risk-adjusted 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
entered later. In addition, the AP considers the evaluation of measures that have just been introduced here
doesn't make sense.
UWV does not read back in the findings that it indicated in August 2019 that the WERKbedrijf is an external employee
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 relate to the period of
the established violation. The AP has, however, mentioned this investigation in section 2.6 of the present
decision.

3.4.2 View of the legal framework and the assessment

The standard that a controller may only take purely organizational measures if he can
demonstrating that it is not possible to take appropriate technical measures does not follow sufficiently from the Dutch DPA,
according to the UWV.
security guidelines from 2013, a CBP case56 and the other sources cited in the report.
The AP does not follow this view of UWV. Firstly, 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 connection with the processing of personal data and on the free movement of those
data, considerations 25 and 46. Secondly, both Article 13 of the Wbp and Article 32 of the GDPR
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 GDPR is thus sufficiently clear, according to the AP. UWV also does not have
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 untenable, now that UWV in December 2018 finally had a technical
measure has been implemented.
The fact that not all measures were equally effective and that incorrect assessments may have been made is possible in the
view
UWV cannot conclude that no or insufficient implementation has been given to the implementation of
appropriate measures. And from the mere fact that there has been some time between the evaluation moment and the
According to the UWV, on the basis of the findings, it cannot be concluded that the introduction of the technical measure
from the eighth data breach, no or insufficient implementation has been given to the implementation of appropriate measures,
if
as a result of insufficient risk management.
The AP does not follow this view of 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 processing in question
guaranteed and guaranteed. The fact that UWV has taken some organizational measures does not change
to the finding that UWV has insufficient risk analyses, technical measures and checks
executed. As UWV itself states, this means that the security measures are not effective
56 https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/arbodienst-handelt-niet-slagen-met-wbp-%C2%A0

goods. In addition, UWV only recommended after the eighth data breach (3 August 2018) to
technical measure, while in October 2016 it was already decided in the District Manager consultation that

the possibility of technical possibilities had to be explored in the short term. In this
In the intervening period of almost 2 years, UWV has thus failed to conduct this investigation.
UWV is also of the opinion that an evaluation did take place after the eighth data breach. Based on view
The UWV therefore does not follow the duration of the detected violation above. According to UWV, after the eighth
data breach, an appropriate level of security is 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 UWV has not periodically updated the measures taken
has fully evaluated and has not sufficiently analyzed the risks beforehand. the FG
moreover, the investigation only took place from November 2018 and the technical measure was initiated by UWV
introduced in 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-adjusted level of security.
In retrospect, with the current knowledge, according to the UWV, the process was not followed to a sufficient extent and there
was insufficient
documented. The Employee Insurance Agency (UWV) notes in this regard that the findings do not show that no interpretation
has been given at all
the various phases of the PDCA cycle or throughout the entire period from 2012 to the end of 2018.
The AP agrees that the findings do not show that no interpretation has been given to the
different phases of the PDCA cycle, but notes that this has not been adequately implemented.
What UWV has documented shows that only the jam 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 security level.

3.5 Conclusion

The AP comes to the conclusion that UWV does not sufficiently provide a security level tailored 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 whereby UWV

period from 2012 to 24 May 2018, has acted in violation of Article 13 of the Wbp and from 25

May 2018 to December 2018 violated Article 32(1) and (2) of the GDPR.

4. Fine

4.1 Introduction

UWV has acted in violation of Article 13 of the Wbp and Article 32(1) and (2) of the GDPR.

The AP uses its authority to fine the UWV for the violation that has been established

for the period from January 1, 2016 (start of AP right to fine) to December 2018. Given the seriousness

of the violation and the extent to which it can be blamed on UWV, the AP considers the imposition of

a fine due. The AP justifies this in the following.

Since in this case there is a continuous violation that has both the Wbp and the AVG

took place, the DPA has checked against the substantive law that applied at the time when the

behavior took place. In this case, this is both Article 13 of the Wbp and Article 32, first and second paragraph, of

the GDPR. These provisions are intended to safeguard the same legal interests and there is no (material)

material regulatory change on this point. Given that the center of gravity of the offense is

at the time of the Wbp, the AP sees reason in this case to align with the 'Finish policy rules'

Dutch Data Protection Authority 2016'.

4.2 Fine policy rules of the Dutch Data Protection Authority 2016

In this case, the AP applies the 'Fine Policy Rules for the Authority for Personal Data 2016' (Fine Policy Rules).

for the interpretation of the power to impose an administrative fine, including determining

of the amount.57 In the Fine Policy Rules, a choice has been made for a category classification and bandwidth

systematically.

Violation of Article 13 of the Wbp is classified in category II. Category II has a penalty bandwidth between €120,000 and €500,000. The AP sets a basic fine within the bandwidth. 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 decreasing or increasing the base amount. It is an assessment of the seriousness of the violation in the specific case, the extent to which the violation can be attributed to the offender be blamed and, if there is reason to do so, other circumstances such as the (financial) circumstances of the offender.

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

58 Fine policy rules, p. 10-11.

4.3.1 Seriousness of the violation

Any processing of personal data must be done properly and lawfully. To prevent organizations with the processing of personal data infringe the privacy of citizens it is of It is very important that they apply a risk-adjusted level of security. 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 for 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 personal

privacy, stricter requirements are imposed on the security of personal data. The
AP has concluded that UWV does not have a sufficiently risk-adjusted security level
guaranteed and guaranteed in the context of sending group messages via the My Work Folder
surroundings.
With regard to the nature of the data, the AP has established that UWV uses a multitude of
processes various personal data of a very sensitive nature, including data about the
health of persons and the citizen service number. Job seekers, the sick and disabled who are legally
are required to register with UWV and to provide their personal data for this purpose,
can trust that UWV properly weighs the risks that these people run.
The impact of a security incident with the personal data processed by UWV can be significant
for a large group of people. For example, it can not sufficiently secure this personal data
lead to stigmatization or exclusion. Now that UWV also processes the BSN, which in practice is a link
of various files is greatly facilitated, there is for persons whose data in
Sonar pose an additional risk to privacy.
In addition to the sensitive nature of the personal data, UWV processes data of an enormous number of citizens.
In the period from 2016 to 2018, UWV processed data on an average of 4,500,000 . in Sonar
persons. All of these people were at risk due to the insufficiently risk-adjusted security level of
UWV. In addition, UWV has already leaked personal data on several occasions. From a total of 15,331
persons, UWV has 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, based on the degree of seriousness of the violation, the AP sees reason to
impose a fine on UWV and increase the basic amount of the fine to € 450,000.

4.3.2 Blame

According to Article 6, second paragraph, of the Policy Rules, the DPA takes into account the extent to which the
offense can be blamed on the offender. If the offense was committed intentionally or
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 'serious culpable negligence' as referred to in Article 66,

fourth paragraph, of the Wbp, if “the violation is the result of seriously culpable negligence, i.e.

is the result of gross, considerably careless, negligent or injudicious act.”59 In this regard

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 findings of the AP that there are serious culpable

negligence. The first four data breaches prompted UWV to make significant adjustments to the process

and to focus on awareness of the risks associated with manual processing. According to

Between the fifth and eighth data breach, UWV has been committed to strengthening this organizational structure

measures (such as workshops). According to the UWV, this means that in the process for sending

group messages in the My Workbook environment has indeed been used for security measures

to improve.

The AP does not follow this view of UWV and motivates this as follows. UWV is obliged to

to use a security level that is appropriate for the nature and scope of the processing operations that UWV

performs. Now that 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 the risks for citizens, taking appropriate measures

security measures and checking and adjusting these measures. For the organizational

measures that have been implemented according to UWV, UWV has not based these measures on

risk assessments and how this has been considered with the possible consequences for those involved. Also has

UWV indicated that it has not checked whether the measures taken after the data leaks

have actually been introduced and evaluated.

The Wbp, the AVG and the CBP guidelines with regard to the security of the processing of
personal data have expressly described that organizations have a risk-adjusted
security level. Partly in view of the sensitive nature and the large size, the UWV may
processing is expected to ensure that it complies with the standards that apply to it and that
acts upon.

In addition, the AP finds it very negligent and negligent that UWV was only granted 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
through 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 health
properly protect personal data.

The AP also considers the fact that UWV has not complied with its own policy rules. Despite
that the policy of UWV indicates that measures must be taken on the basis of explicit
risk assessments as part of a PDCA cycle, UWV has not and insufficiently taken into account
with the risks and consequences for job seekers. In addition, UWV did not have a
technical measure was introduced while UWV had already decided on 20 October 2016 to
to start research into 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.

not checked whether the measures that were taken as a result of the data leaks were
actually implemented in the organization. The violation is therefore the result of coarse and

Significant carelessness by the UWV.

In the opinion of the AP, it appears from all of the above that UWV is grossly, considerably carelessly or acted negligently, resulting in serious culpable negligence on the part of UWV. In view of the circumstances of this case and the criterion of grossly culpable negligence under the Wbp, however, the AP sees no reason to lower or further increase the fine.

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 does not lead to a disproportionate outcome in view of the circumstances of the specific case.

The AP is of the opinion that, given the seriousness of the violation and the extent to which it can be attributed to the 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 the risks for citizens, the lack of have appropriate security measures and failure to monitor and evaluate these measures after all, led to an insufficiently risk-adjusted security level. The violation has In addition, it took almost 3 years, during which the privacy of 4,500,000 people was insufficiently guaranteed.

In view of all the circumstances of this case, the AP sees no reason to set the amount of the fine on the basis of the proportionality and the circumstances mentioned in the Fine Policy Rules, to the extent applicable in in the present case, further increase or decrease.

4.4 Conclusion

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

61 For the motivation, see paragraphs 4.3.1 and 4.3.2.

May 31, 2021

5. Operative part

The AP submits 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 (four hundred and fifty thousand euros).62

Yours faithfully,

Authority Personal Data,

w.g.

drs. C.E. Mur

board member

Remedies Clause

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

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

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

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

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

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

title of your letter 'objection'. In your notice of objection, write at least:

 Your name and address

 The date of your notice of objection

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

attach

 The reason(s) why you disagree with this decision

 Your signature

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

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. Policy of UWV

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

In addition, 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 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 stated: included the following: “When processing and storing personal data, the required technical and organizational security measures selected and implemented 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, the UWV makes policy document, valid from December 2015 until 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 one's own line

reported, in accordance with the own agreements. From the central monitoring of the IB&P risks, the

organizational units to report on the UWV-wide top IB&P risks.

The organizational units have the following responsibilities in this regard:

• Reporting from the executive 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 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 the file “Document” with the answer to question 4 under

data breach 1).

64 Ditto.

65 See file 38 (Excel file, appendix 7 (file “UWV BZ IBP Sectie A Legal Framework v100.docx”, p. 11) and appendix 10 (file "UWV BZ IBP Section A Legal Framework v102 (AVG version)", p. 12). These attachments are part of file “Document” in reply to

question 4 under data breach 1).

66 See file 38 (Excel file, appendix 7 (file “UWV BZ IBP Sectie A Legal Framework v100.docx”, p. 11) and appendix 10 (file "UWV BZ IBP Section A Legal Framework v102 (AVG version)", p. 12). These attachments are part of file “Document” in response to

question 4 under data breach 1).

67 See file 38 (Excel file, appendix 9 (file “UWV BZ IBP Sectie C Borging BIR Control v200” which is part of

file “Document” for answer to question 4 under data breach 1, p. 7-8)).

Date

May 31, 2021

Our reference

• 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 IS&P risks. For the

To obtain 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 IS&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 to recalibrate the UWV-wide risks and (BIR) improvement plans;

• Providing substantive support on the improvement plans and actions to be carried out;

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

2. Practice within UWV

2.1 Weighing risks in practice

With regard to the performance of risk analyses, UWV states that it: "is an organization that in general

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

approach with concrete improvements instead of bulky reports. Documents that we, for example, use as a 'risk analysis'

can be termed 'research' by the department which means either understandably but

the wrong impression can arise that we are not complete".69

When asked whether prior to the decision in 2012 to send group messages in a way other than Outlook,

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

workbook no risk analysis per se made".70

When asked how UWV determined in 2012 that sending group messages via the My Work Folder environment is an acceptable risk, which security measures have been considered and how this is considered has been created, 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. In addition, unlike with sending via outlook- messages sent once will be deleted if a message is sent incorrectly. UWV sees therefore, the workbook as one of the safe channels for exchanging data and messages”.71

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

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

70 See file document 98 (Reply by UWV, file "Additional questions AP2110", p. 2, appendix 4 (file “Explanation note meeting of the WERKbedrijf Management Team”) and appendix 5 (file “28 BV 06 Decision document prohibiting the use of group email via Outlook”)).

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

When asked whether the specific data breaches have prompted a risk analysis UWV states: “UWV and in particular the WERKbedrijf division, as a result of the four leaks in 2016, has risk analysis performed. This risk analysis can be found in the document: 'Voorlegger DMO WERKbedrijf' and its appendices, containing guidelines for employees”.72 In this October 2016 submission, the following is stated included: “To cope with the unrest and disrupt the service as little as possible, but at the same time In order to conduct a thorough analysis of where we run risks in our customer communication, we propose the following measures for (…)”.73

When asked whether a risk analysis was 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 following the data leaks in August and

September 2016. See the submission - a proposal for decision-making - of the 4th quarter 2016 of the BSO

WORK company with decisions to be taken/impact analysis/measures and conclusions and recommendations. In addition in

the

annex a guideline for 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. Following the two leaks in 2018, the Board of Directors has appointed the Officer

Data protection requested to launch an investigation”.74

When asked why it saw no need to carry out a risk analysis after the leak in 2017, UWV said:

the following: “UWV has weighed up and, of course, also assigned weight to the rights and

freedoms of those involved. By now, with today's knowledge, this trade-off may be different”. 75 UWV has

upon request, no documents were provided in which the assessment made at the time is recorded.

With regard to data leaks five to eight, UWV reports: “The risk of more leaks was considered low

and measures from October 2016 seemed to work satisfactorily, as we explained earlier in the response to

the information request. At that time, a number of other ICT measures in the systems had a high priority.

In retrospect, that was a wrong estimate and technical measures should have been taken sooner.”76

UWV has not substantiated what the estimate was based on that the risk should be considered low

considered.

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

As a result of this data breach, an investigation was conducted into export functionality within the workbook. In addition (sic)

performs

the Data Protection Officer (DPO) on behalf of the Board of Directors is currently carrying out a risk analysis on

Sonar”.77

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

73 See, among other things, file 38 (Excel file, appendix 27 (file “Microsoft Word 97-2003 document” in answer to 11 under

data breach 1

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

74 See, among other things, file 38 (Excel file, answer to 11 under data breach 1 to 4).

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

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

77 See, among other things, file 38 (Excel file, answer to 11 under data breach 7).

2.2 Measures, checks 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

and that it has decided to take measures.78

UWV reported with regard to the measures after the four data breaches in 2016: “Then immediately

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

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

had decided on the following temporary measures, which relate to the sending of messages with

attachments via the My Work Folder environment to multiple job seekers at the same time:80

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

from the WORK company via the following WORK message:81

78 See, among other things, file 38 (Excel file, answer to question 18 under data breach 1 to 4).

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

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

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

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

Date

May 31, 2021

Our reference

[CONFIDENTIAL]

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

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

About the temporary measures mentioned on the previous page, UWV indicates that they will be applied as soon as possible

entered into force after September 28, 2016. UWV also states that 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 the moment.83 However, 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 (Reply by UWV, appendix, answer to question 2).

Date

May 31, 2021

Our reference

[CONFIDENTIAL]

Measures proposed in October 2016

In the submission of October 18, 2016, which was prepared in preparation for the District Managers' Consultation

(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 measures below, in order to:

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)).

[CONFIDENTIAL]

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

next decided:86

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

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

including an investigation into concrete technical measures - to be tackled 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" is

88 As can be seen below, this - undated - Guideline contains basic principles for

secure communication:89

86 See file document 102 (Reply by UWV, appendix 1 (file “42DMO-A04. Decisions and action points overview 20 Oct. 2016",

p. 3

and 4)).

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

88 See file 38 (Excel file, appendix 33 (file "161020 Appendix A Data leaks WB", which is part of file "Microsoft

Word document" for answer to question 15 under data breach 1)).

89 See file 38 (Excel file, appendix 33 (file "161020 Appendix A Data leaks WB", which is part of file "Microsoft

Word document" for answer to question 15 under data breach 1)).

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

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

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

WERKbedrijf that operate throughout the country, regional offices can to a certain extent give their own interpretation to central policy, for example with awareness campaigns.”91 UWV also reports on this: “There is no formal protocolled procedure within UWV in 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 amount of decisions that UWV makes”.92 UWV states in response to the actual findings, however, that it would have checked whether the measures taken were in practice have been brought.93 UWV has not substantiated this statement with documentation.

To the question whether and in what way the measures taken by UWV as a result of the first four data breaches had decided to be evaluated, what the results of that evaluation were and whether the desired effect of that measures had been achieved, UWV reports: “No, given the relatively limited number of leaks in 2017 compared to the number of leaks from 2017 in absolute terms.

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

UWV states the following with regard to the way in which it carries out evaluations: "There is no formal protocolled evaluation process after each of the seven data breaches. That is not the way UWV works in all cases works. The departments involved concluded in close consultation for some time that the measures taken in 2016 measures were sufficient. Unfortunately, this conclusion turned out to be incorrect."96 UWV states in response to the factual findings, however, that evaluations have been carried out with regard to 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 increase awareness of the sending messages via the My Workmap environment.98 In that context, after the data breach on 20 July 2017 The following WORK message has been sent by UWV to managers of the WERKbedrijf:99

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

92 See file documents 65 and 66 (Reply 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, among other things, file 38 (Excel file, answer to question 18 under data breach 6).

95 See, among other things, file 38 (Excel file, answer to question 18 under data breach 1 to 4).

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

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

98 See, among other things, file 38 (Excel file, answer to question 13 under data breach 5).

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

UWV also states with regard to this data breach: "As a result of this leak, UWV/WERKbedrijf has adopted the 'Safe communicating'" and UWV has issued the “Guideline for safe communication at WERKbedrijf” with the answers to questions about the fifth data breach have been added.100 Based on what is stated on page 31, to follow, however, that this directive had already been drawn up after the fourth data breach. And as mentioned before, UWV has provided no proof 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 after this leak, no additional technical measures to take was mainly a full release agenda, coupled with a far-reaching change assignment for WERKbedrijf”.101 UWV has not provided any documents in which this decision is contained.

With regard to the question of how it has been checked that the aforementioned measures are also have actually been carried out answered that UWV and WERKbedrijf do not have as such checked whether measures taken in response to data breaches have actually been implemented entered.102

100 See, among other things, file 38 (Excel file, answer to question 18 under data breach 5).

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

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

To the question whether and how the measures decided by UWV after the fifth data breach have been 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

With regard to the way in which it carries out evaluations of measures, UWV states the following: “There is no formally protocolled evaluation process after each of the seven data breaches. That is not the way UWV works in all cases. The departments involved concluded in close consultation for some time that the measures taken in 2016 measures were sufficient. Unfortunately, this conclusion 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 assertion that an evaluation would have taken place is not substantiated with documentation from which the evaluation actually appears.

Sixth to ninth data breach (2018)

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

"-Workshop Prevention Data Leaks

This is a workshop aimed at increasing awareness about working with personal data and the conducting risk analyses. The workshop was transferred to representatives from all over the world via the 'train the trainer' labor market regions, who subsequently rolled out the training across the branches.

- Common toolkit page on DWU

Partly as a result of the introduction of the GDPR, the toolkit page of the IB&P has been further expanded and there is a lot of material offered. This is partly to support the above workshop.

- Step-by-step plan Safely Sharing Personal Data

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

- Attention from management

The Information Security & Privacy and Security advisory meeting 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'

- Rollout SLIM

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

Technical measure:

103 See, among other things, file 38 (Excel file, answer to question 18 under data breach 5).

104 See file documents 65 and 66 (Reply 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 (Reply by UWV, appendix 3 (file "Question 7 appendix 2")).

107 See, among other things, file 38 (Excel file, answer to question 13 under data breach 6 and 7).

Date

May 31, 2021

Our reference

[CONFIDENTIAL]

Attachments block

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 on the basis of the technical measure of which it can be established how the above-mentioned measures are secured 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 step-by-step plan is dated April 26, 2018 and therefore drawn up after the seventh data breach. UWV states about this: "In the light of the entry into force of the AVG, the old directive 'Safer Digital Communication' has been replaced by the directive 'Step-by-step plan Safely sharing personal data'.108 This step-by-step plan looks like this:

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

The step-by-step plan was published on 1 May 2018 via the newsletter to employees of the WERKbedrijf communicated:109

When asked whether there are technical measures in place 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 several organizational and process-related measures have been implemented. 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 previously outlined backlog of 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 20 August 2018 how the data breach could have happened take place and how this specific data breach was handled towards the data subjects. This analysis is described in a document, which includes 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 (Reply by UWV, appendix, p. 1, answer to question 1).

111 See file 38 (Excel file, appendix 42 (file “Microsoft Word document" in answer to question 18 under data breach 7), p. 3).

Our reference

[CONFIDENTIAL]

In addition, UWV has stated about the above-mentioned analysis: “First of all, WERKbedrijf in September 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 on how to deal with bulk messages via the Workbook to prevent this type of leak. More research in the sense of a comprehensive report is not necessary here 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- viz. a to build a block in the Workbook so that, among other things, Excel files can no longer be sent, which means December has 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 prevent:113

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

113 See file 91 (Reply by UWV, appendix 4 (file "QRC Sonar Send Group Message to Werkmap 22072013", p. 1)).

Date

May 31, 2021

Our reference

[CONFIDENTIAL]

At the first point in the above-mentioned passage from QRC group messages of September 3, 2018 states that the export lists for sending group messages must first be prepared by the employees be cleaned by deleting data from the file. As a result, only the row ID remains about. Furthermore, this version of the QRC group messages states that the 4-eye principle must be used become. In previous versions of the QRC group messages provided, these instructions about the

cleaning and not including the row ID and the 4-eye principle.

On September 4, 2018, the AP had a telephone consultation with the DPO of UWV. In it is under others considered whether technical measures had been introduced in the meantime. In that conversation the DPO has indicated that, to the best of his knowledge, there are currently no technical measures had been introduced. He also indicated that the four-eye principle had been introduced. He found that the method is inherently insecure now that 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 guarantees.114

As a result of the eighth data breach, the DPO of UWV has, at the request of the Board of Directors of UWV has conducted an investigation and has described this in the “FG report of findings: Datalek Alkmaar” of 30 November 2018.115 The DPO presented the results of that investigation to the Board of Directors on 22 January 2019. Werkbedrijf Board and Management Board presented.116 This presentation included, among other things:

114 See file 22 (Phone note FG UWV).

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

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

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

(…)

“Plasters Paste: Process agreements are not ‘hard’ enforced” (…)

“Policy does not affect the workplace:

 Understanding process agreements

 Awereness does not reach all employees”

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

With regard to the question of how it has been checked whether measures have actually been taken, UWV has entered answer that UWV and WERKbedrijf have not checked as such whether measures that have been taken in response to data breaches have actually been introduced.118

To the question whether UWV had commissioned external parties to investigate the data breaches, answers UWV with regard to the first eight data breaches: “UWV saw no 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 has stated with regard to the eighth data breach: “UWV Internal investigation by Administrative Affairs commissioned by FG, whereby external expertise was obtained from a consultant”.120

UWV states the following with regard to the way in which it carries out evaluations: “There is no formal protocolled evaluation process after each of the seven data breaches. That is not the way UWV works in all cases works. The departments involved concluded in close consultation for some time that the measures taken in 2016 measures were sufficient. Unfortunately, this conclusion 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 This assertion that an evaluation would have taken place is not substantiated with documentation from which the evaluation actually appears.

117 See file 38 (Reply by UWV, letter), file 38 (Excel file, answer to question 13 under data breach 6 and 7), file documents 65 and 66 (Reply by UWV, p. 2 and appendix, p. 1, answer to question 2) and file document 81 (Reply by UWV, appendix 1 (file "Answer questions AP August 2019", answer to question 17)).

118 See, among other things, file 38 (Excel file, answer to question 17 under data breach 1 to 7).

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

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

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

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