Registered

[CONFIDENTIAL]

Date

November 6, 2018

Our reference

[CONFIDENTIAL]

Contact

[CONFIDENTIAL]

Subject

Decision to impose an administrative fine

Authority for Personal Data

PO Box 93374, 2509 AJ The Hague

Bezuidenhoutseweg 30, 2594 AV The Hague

T 070 8888 500 - F 070 8888 501

authoritypersonal data.nl

Dear Sirs [CONFIDENTIAL],

The Dutch Data Protection Authority (AP) has decided to inform your clients Uber B.V. (UBV) and Uber Technologies, Inc. (UTI) jointly impose an administrative fine of € 600,000, because UBV and UTI, as (jointly) responsible on November 15, 2016, at least within 72 hours at the latest after UTI was notified of the data breach on November 14, 2016, the AP and notify data subjects of the data breach.

The report to the AP first took place on November 21, 2017. On that same day, Uber issued a published a news item about the data breach on its website. The AP and those involved are not with that immediately notified of the data breach. This is a violation of Article 34a, first and second paragraph, of the Personal Data Protection Act (Wbp), as it applied at the time.

The decision is explained in more detail below. Paragraph 1 presents the facts on which it is based

depend on the decision. Section 2 describes the legal framework. In section 3, the AP assesses her competence, responsibility for data processing, violations and serious culpable negligence. Section 4 details the amount of the administrative fine. Section 5 contains the operative part and the remedy clause.

1

Date

November 6, 2018

Our reference

[CONFIDENTIAL]

Legal entities involved

Facts and process

1.

1.1

Uber BV

UBV is one of the Mr. Treublaan 7, (1097 DP) Amsterdam, a private company with its registered office. UBV was founded on October 24, 2012 and is registered in the register of the Chamber of Commerce under number 56317441. UBV is an indirect wholly owned subsidiary of UTI.

Uber Technologies Inc

UTI is located at 1455 Market Street, San Francisco, United States. UTI is the final one parent company of a group of dozens of companies, including UBV.

UTI and UBV are hereinafter jointly referred to as "Uber" or as the "Uber Group".

1.2

On November 21, 2017, UBV reported1 a data breach to the AP.

Process flow

As a result of that notification, the AP is an ex officio authority pursuant to Article 6o, first paragraph, of the Wbp investigation started. In that context, on 23 November 2017, a first written request for information was made

sent to UBV. Subsequently, several requests for information followed. Uber followed suit

datum.

The results of the investigation into the notification of the aforementioned data breach are included in the report that

was adopted by the director of Policy, International, Strategy and Communication on 1 June 2018.2

On June 15, 2018, the AP sent Uber an intention to impose an administrative fine

due to violation of Article 34a, first paragraph and second paragraph, of the Wbp.

On July 3, 2018, Uber gave its opinion in writing on the intention to impose a

administrative fine and the report drawn up for it.

On July 11, 2018, a hearing took place at the offices of the AP, in which Uber also verbally

explained her point of view.

On September 14, 2018, the AP sent the report of the hearing to Uber. By letter from

On September 27, 2018, Uber made its comments on the report known to the AP.

In a letter dated October 22, 2018, Uber's authorized representative sent the AP a further document.

1 Attribute [CONFIDENTIAL]

2 Investigation report [CONFIDENTIAL]

Date

November 6, 2018

Our reference

[CONFIDENTIAL]

Services Uber

Processor Agreement

Storage of (personal) data in the United States

1.3

The Uber group offers a service that makes it possible for users of that service to book taxi rides

can be ordered via, among other things, an application (the Uber app). Users of the Uber app who want a taxi ride

orders (riders) are linked to drivers (drivers) who order via another application of the Uber-
concern customers (the Uber Driver app). Uber drivers use their own car for it
offering rides, are not employed by Uber and may not meet the demand for rides from Uber riders
accept or refuse.
To use the Uber apps, both as a rider or as a driver, it is necessary to have an account
to create. For this it is mandatory to provide first and last name, telephone number and e-mail address
to give. The purpose of processing this data is, among other things, to bring together demand and
offer to/from taxi rides and the processing of payments for those taxi rides.

1.4

On March 31, 2016, UBV and UTI concluded a Data Processing Agreement.
In it, UBV and UTI have agreed that UBV is responsible for the processing of
personal data that it collects and processes from data subjects outside the United States of America
(United States) and that UTI processes that data as a processor on behalf of UBV.

1.5

The data of drivers and users of the Uber app outside of the United States will be
forwarded from the Netherlands to the United States. There they are stored on servers of UTI
in the United States. It has also emerged that UTI has a processor agreement for the use of data
storage capacity/servers (AWS S3) has been contracted with Amazon. The purpose of that storage is to create
backups of that (personal) data.

1.6

On November 14, 2016, UTI was made aware of a vulnerability in its data security. On
that date the then [CONFIDENTIAL] of UTI received an e-mail message from a person who received the
[CONFIDENTIAL] informed that he and his team (reporter/reporters) have identified a major vulnerability in the
data security of the Uber group.
The reporter has had access to AWS S3 storage in the period from October 13, 2016 to November 15, 2016
of the Uber group through credentials stored in a private GitHub

repository of the Uber group. Amazon's servers contained "rider" (customer) and "driver"

(driver) data stored. This concerns the following personal data:

1 user ID;

2 Driver ID;

3 First and Last names;

4 Email address;

5 Mobile number;

Data leak and report to AP

Date

November 6, 2018

Our reference

[CONFIDENTIAL]

6 Last confirmed mobile number;

7 Nickname;

8 Driver's license number;

9 Email receipt;

10 token;

11 Mobile Token;

12 Email Token;

13 [CONFIDENTIAL];

14 [CONFIDENTIAL];

15 Location of signup (lattitude/longtitude);

16 Signup “shape”;

17 Location;

18 Inviter ID;

19 InviterUUID;

20 Recent fare splitter ID;

21 Meta field;

22Notes;

23 Driver payment statements;

24 license plate numbers;

25 NYC UC numbers;

26 User rating;

27 Driver rating;

28 Professionalism score;

29 City knowledge score;

30 Banned;

31 Fraud rate.

On November 15, 2016, UTI fixed the data breach.

The data breach prompted UTI to call in [CONFIDENTIAL], a forensic expert. It

request to this effect was made on 18 October 2017. [CONFIDENTIAL] has investigated to what extent the

reporters had access to data from the Uber group that was on Amazon servers at the time

stored. [CONFIDENTIAL] has recorded its findings in a report.3 This has been established

the data breach involved 57,383,315 Uber users, of which 25,606,182 were American and

31,777,133 non-U.S. The information from UBV shows that approximately 174,000 Dutch Uber drivers

users have been affected by the data breach. It appears from the research carried out by [CONFIDENTIAL].

that 31 types of personal data were involved in the data breach.

On October 25, 2017, UBV's [CONFIDENTIAL] became aware of what Uber calls an “IT

security incident in 2016, that it was being investigated, and that it could potentially create a media cycle.”

3 Report dated 10 January 2018, [CONFIDENTIAL].

Date

November 6, 2018

Our reference

[CONFIDENTIAL]

On November 4, 2017, a meeting took place between UTI and UBV. During this discussion

UTI has indicated that there was a security incident.

On November 21, 2017, a news post was published on Uber's website by the current CEO of

UTI in which the public is informed about the data breach.4 On the same day, UBV reported

a data breach to the AP.

2. Legal framework

At the time of the data breach from October 13, 2016 to November 15, 2016 and at the time of the notification by

UBV to the AP on November 21, 2017, the Wbp applied, including the data breach notification obligation as laid down

in Article 34a, first and second paragraph, of the Wbp. The Wbp, which formed the implementation of a guideline

95/46/EC5, was repealed on 25 May 2018.6 On that day, the General Regulation

Data Protection (GDPR) has become applicable7 and the General Regulation Implementation Act

Data Protection (UAVG) entered into force.8

Subsection 2.1 will first describe the legal framework under the Wbp, insofar as relevant, and

explained. Subsection 2.2 then describes the legal framework under the GDPR, where relevant,

described.

2.1

2.1.1

Article 1, preamble and under a, of the Wbp stipulates that personal data is any data concerning a

identified or identifiable natural person. The concept of personal data must be broadened

conceived. To determine whether a natural person is identifiable “all means must be considered

which may be reasonably assumed to have been obtained by the person responsible for the processing

be used by any other person to identify said person”.9

Article 1, preamble and under b, of the Wbp stipulates that the processing of personal data is any act

or any set of acts related to personal data, including in any case the

collecting, recording, organizing, storing, updating, changing, retrieving, consulting, using,

providing by transmission, distribution or any other form of making available,

Processing of personal data

Wbp

4 See https://www.uber.com/newsroom/2016-data-incident/

5 Directive of the European Parliament and of the Council of 24 October 1995, Official Journal of the European Communities,

23

November 1995, No. L 281/31 (the so-called Privacy Directive).

6 In Article 51 of the General Data Protection Regulation Implementation Act (UAVG) – which came into effect on

of 25 May 2018 – states that the Wbp will be withdrawn.

7 Article 99, second paragraph, of the GDPR stipulates that the GDPR applies from 25 May 2018.

8 By Royal Decree of 16 May 2018 (Staatsblad 2018, 145) the time for determining the entry into force of the UAVG

adopted on 25 May 2018. This decision is based on Article 53 of the UAVG, whereby the entry into force of the UAVG on a

time to be determined by Royal Decree has been made possible.

9 Recital 26 Directive 95/46/EC (Directive on the Protection of Personal Data).

Date

November 6, 2018

Our reference

[CONFIDENTIAL]

Scope of application Wbp

bringing together, associating with each other, as well as shielding, erasing or destroying

facts.

2.1.2 Responsible

Article 1, preamble and under d, of the Wbp stipulates that the controller is the natural person, legal entity or any other body or governing body that, alone or jointly with others, has the purpose of and determines the means for the processing of personal data.

The Court of Justice of the European Union (CJEU) has confirmed in a recent judgment that any joint responsibility for certain data processing does not detract from the individual responsibility of one of the (joint) controllers.10

2.1.3

Article 4(1) of the Wbp stipulates that the Wbp applies to the processing of personal data in the context of activities of an establishment of a controller in the Netherlands.

Article 4, second paragraph, of the Wbp stipulates that the Wbp applies to the processing of personal data by or on behalf of a controller who does not have an establishment in the European Union, using automated or non-automated means located in the Netherlands unless these means are only used for the transmission of personal data.

2.1.4

Article 13 of the Wbp stipulates that the responsible person has appropriate technical and organizational implements measures to protect personal data against loss or against any form of unlawful processing. These measures guarantee, taking into account the state of the art and the costs of implementation, an appropriate level of security in view of the risks posed by the processing and the nature of the data to be protected. The measures are also on it aimed at preventing unnecessary collection and further processing of personal data.11

2.1.5 Data breach notification obligation

As of 1 January 201612, article 34a, paragraph 1, of the Wbp stipulates that the controller must inform the Board (read: informs the AP) immediately of a security breach, as referred to in Article 13 of the Wbp, which Security Obligation

10 CJEU, C□131/12 (Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEP)), 13 May 2014, para 40. The Lawyer-

General Bot (AG) of the CJEU has argued in a recent Opinion that "joint responsibility" within the meaning of the
The Directive can be interpreted broadly, in the sense that various variants and divisions of tasks are possible and also that
when determining
the division of responsibilities in a legal sense the way in which entities actually cooperate in practice a
is the decisive criterion. See: Opinion AG Bot, Case C□210/16 (Wirtschaftsakademie Schleswig-Holstein), 24 October 2017,
par. 46-
51 and the subsequent judgment CJEU, C□210/16, 5 June 2018, ECLI:EU:C:2018:388.
11 The AP (then the Personal Data Protection Authority) has further details in its Guidelines for the protection of personal data
has elaborated what is meant by 'appropriate technical and organizational security measures'. Thereby
connected to standards, methods and measures that are customary in the field of information security. See CBP
Guidelines for the Protection of Personal Data, February 2013, URL:
https://autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-publishes-
guidelines-security-of-personal data.
12 Royal Decree of 1 July 2015 (Stb. 2015, 281).

Date
November 6, 2018
Our reference
[CONFIDENTIAL]
Administrative fine
leads to a significant risk of serious adverse consequences or has serious adverse consequences for
the protection of personal data.
Article 34a, second paragraph, of the Wbp stipulates that the controller must immediately inform the data subject
of the infringement, referred to in Article 34a, first paragraph, of the Wbp, if the infringement is probable
will have unfavorable consequences for his privacy.
The AP has further elaborated in its Policy Rules on the obligation to report data breaches how those responsible

must give substance to the data breach notification obligation, and provide tools for those responsible to determine whether they have to report certain security incidents under the data breach notification obligation to the AP to report.13 The Policy Rules on the obligation to report data breaches also contain details of the obligation to report data subjects. The Policy Rules on the obligation to report data breaches stipulate, among other things, that 'immediately', as intended

in Article 34a, first paragraph, of the Wbp, means notification within 72 hours.

2.1.6

Article 66, second paragraph, of the Wbp stipulates, insofar as relevant, that the AP can impose an administrative fine imposing a maximum of the amount of the fine of the sixth category of Article 23, fourth paragraph, of the Criminal Code with regard to violation of the provisions of Article 34a of the Wbp. Article 23, seventh paragraph, of the Criminal Code applies mutatis mutandis.

Article 66, third paragraph, of the Wbp stipulates, insofar as relevant, that the AP does not impose an administrative fine due to violation of the provisions of or pursuant to the provisions referred to in Article 66, second paragraph, of the Wbp articles, then after it has issued a binding instruction. The AP can give the offender a time limit within which the instruction must be followed.

Article 66, fourth paragraph, Wbp stipulates that the third paragraph does not apply if the violation committed intentionally or as a result of grossly culpable negligence.

2.2

2.2.1 Notification of a personal data breach to the AP

Article 33, first paragraph, of the GDPR stipulates that if a personal data breach has occurred occurred, the controller notifies it without undue delay and, if possible, at the latest 72 hours after becoming aware of it, to the person referred to in Article 55 competent supervisory authority, unless it is unlikely that the breach related to personal data poses a risk to the rights and freedoms of natural persons. If the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by a justification for the delay.

13 Policy rules 'The obligation to report data breaches in the Personal Data Protection Act (Wbp)' of 8 December 2015 (Stcrt. 2015, no. 46128).

Article 33, paragraph 2, of the GDPR stipulates that the processor shall be the controller without unreasonable delay informs as soon as he becomes aware of a breach in connection with personal data.

2.2.2 Communication of a personal data breach to the data subject

Article 34, paragraph 1, of the GDPR stipulates that when the personal data breach occurs is likely to pose a high risk to the rights and freedoms of natural persons, the controller, the data subject shall immediately report the personal data breach shares.

2.2.3

Article 83, paragraph 1, of the GDPR stipulates that each supervisory authority must ensure that the administrative fines imposed under this Article for the offenses referred to in paragraphs 4, 5 and 6 reported infringements of this Regulation are effective, proportionate and dissuasive in each case.

Administrative fine

Judgement

Article 83, paragraph 4, of the GDPR stipulates that infringements of Articles 33 and 34 are subject to an administrative fine can be imposed up to € 10,000,000 or, for a company, up to 2% of the total worldwide annual turnover in the previous financial year, if this figure is higher.

3.

In this section, subsection 3.1. first discussed the authority of the AP. Thereafter

responsibility for data processing is set out in sub-section 3.2. The

Violation of article 34a, first paragraph, of the Wbp is established in subsection 3.3. The violation

of Article 34a, second paragraph, of the Wbp is determined in subsection 3.4, after which in subsection 3.5

seriously culpable negligence.

3.1

3.1.1

From October 13, 2016 to November 15, 2016, there was a data breach at the Uber group.14 Of this, UTI was

November 14, 2016 notified. On November 21, 2017, UBV reported this data breach to the AP,

after which the AP - pursuant to Article 60 of the Wbp - started an investigation. On November 23, 2017

the AP has sent a first written request for information to UBV. The final the

research findings of the study are included in the report dated June 1, 2018. That report and

Uber's views on the intention to impose an administrative fine have resulted

in the present decision. The AP is authorized to take enforcement action in response to the aforementioned data breach

and thereby take this decision. Then she explains.

Competence of the Dutch Data Protection Authority

Period of the conduct

14 This is substantiated in subsection 3.3 'obligation to report data breach to AP'.

Date

November 6, 2018

Our reference

[CONFIDENTIAL]

3.1.2 GDPR as a basis for a fine

At the time of the data breach from October 13, 2016 to November 15, 2016 and at the time of the notification by

UBV on 21 November 2017, the Wbp applied. The Wbp, which implemented Directive 95/46/EC15, is withdrawn on 25 May 2018.16 On that day the GDPR also became applicable17 and the UAVG in entered into force.18

The AVG replaces Directive 95/46/EG19 and the Wbp. Where the GDPR gives room for further rules these are laid down in the UAVG. According to the recitals to the GDPR, the objectives and principles of Directive 95/46/EC maintained.20 Both Directive 95/46/EC and the Wbp and the AVG aim to protect the fundamental rights and freedoms of natural persons related to processing activities and the free movement of personal data within the Union guarantees. The material standards to which the processing of personal data under the regime of the GDPR, have - broadly speaking - also remained the same as those from Directive 95/46/EC and the Wbp.

In this case it is important that there is a obligation to report data leaks21 and that failure to comply with the obligation to report is subject to a fine. In the Wbp, the obligation to report laid down in 34a, first and second paragraph, of the Wbp and in the AVG in Article 33, first paragraph and Article 34, first paragraph. These provisions aim to safeguard the same legal interests. The authority to imposing an administrative fine for a data breach is regulated in the Wbp in Article 66, second paragraph, of the Wbp and in the AVG in Article 58, second paragraph, opening lines and under i, read in conjunction with Article 83, fourth paragraph of the GDPR. There is no question of a (substantial) material change to the regulations. Also there is no other way of thinking about the criminal nature of the obligation to report as such.22 This is the case of an uninterrupted legal order. This means that, to ensure the continuity of the legal order, for conduct that - as in the present case - took place under the regime of the directive 95/46/EC and the Wbp, compliance must be ensured with the rights and obligations as they applied under that regime.23

15 Directive of the European Parliament and of the Council of 24 October 1995, Official Journal of the European Communities, 23 November 1995, No. L 281/31 (the so-called Privacy Directive).

16 Article 51 of the UAVG – which came into effect on 25 May 2018 – states that the Wbp is repealed.

17 Article 99, second paragraph, of the GDPR stipulates that the GDPR applies from 25 May 2018.

18 By Royal Decree of 16 May 2018 (Staatsblad 2018, 145) the time for determining the entry into force of the UAVG is adopted on 25 May 2018. This decision is based on Article 53 of the UAVG, whereby the entry into force of the UAVG on a time to be determined by Royal Decree has been made possible.

19 Article 94 of the GDPR repeals Directive 95/46/EC with effect from 25 May 2018.

20 Cf. recital 9 of the GDPR.

21 Although Directive 95/46/EC did not contain any regulations on a data breach notification obligation, the legislative history regarding the
introduction of the reporting obligation in the Wbp that the legislator, with reference to the recognition by the European Union of the
protection of personal data as a fundamental right, as evidenced by Directive 95/46/EC, a regulation for
regarded the obligation to report data breaches as an overriding requirement of public interest. The legislative history also shows that with
the introduction of the reporting obligation was intended to prevent the processing of personal data in violation of Directive 95/46/EC
(Parliamentary Documents II 2012/13, 33 662, no. 3 Reprint, p. 14.)

22 There is, however, a change in the sentencing.

23 In this context, the AP refers to European jurisprudence in this regard. cf. CJEU 29 March 2011 on ThyssenKrupp (C-352/09 P), CJEU 18 July 2007 regarding Lucchini (C-119/05) and the judgment of the Court of Justice of 25 February 1969 regarding
Klomp (Case 23-68).

Date

November 6, 2018

Our reference

[CONFIDENTIAL]

In a case where the continuity of the legal order is at issue, insofar as relevant here,

tested against the substantive law as it applied at the time when the conduct24 took place.25 In this

the case is the Wbp, more specifically article 34a, first and second paragraph. This also means that is

affiliated with the 'more favorable' penalty regime for the offender under the Wbp, compared to the AVG.26

After all, under the GDPR, a violation of the reporting obligation can be fined up to €10,000,000 or, if

this is higher, up to 2% of the total worldwide annual turnover27, while under the Wbp regime this is, in view of

Article 66, second, third and fourth paragraph, of the Wbp, was in principle a maximum of € 820,000.28

Pursuant to the GDPR, the obligation to report can be fined on the basis of Article 58, paragraph 2, preamble and

under i, viewed in conjunction with Article 83, fourth paragraph, under a. As the AP explains in more detail in this decision,

would the present conduct - and which conduct in this Decree constitute a violation of Article 34a, first and

second paragraph, of the Wbp is qualified - if it would have occurred under the regime of the

AVG have resulted in a violation of Articles 33, first paragraph and 34, first paragraph, of the AVG.

3.1.3 Wbp as a basis of jurisdiction; transitional law UAVG

Article 48, eighth paragraph, of the UAVG provides for transitional law. Pursuant to that provision

legal procedures and legal proceedings where the Dutch Data Protection Authority29 preceded

is involved in the entry into force of the UAVG, the law applies as it applied before

to the entry into force of the UAVG.

Insofar as conducting an investigation is a legal procedure as referred to in Article 48, paragraph 8, of the

UAVG then also derives the power to impose an administrative fine from the Wbp. It

then this concerns a legal procedure in which the AP, prior to the entry into force of the UAVG -

so before May 25, 2018 - got involved. This legal procedure continues after the withdrawal of the

Wbp and the application of the GDPR and the entry into force of the UAVG. Also by the AP

report drawn up on 1 June 2018 and (the procedure that led to) the present decision are part

24 It should be noted that an act also includes an omission, such as in the present case not immediately reporting a

data breach.

25 Again, reference is made to European jurisprudence in this area. cf. CJEU 29 March 2011 on ThyssenKrupp (C-

352/09 P), paragraph 79 and EC Court of First Instance of 12 September 2007 in González y Díez, SA, SA (T-25/04), paragraph 59.

26 In Article 5:46, fourth paragraph, of the Awb, Article 1, second paragraph, of the Criminal Code applies mutatis mutandis declared. Pursuant to Article 1, second paragraph, of the Penal Code, changes in legislation after the time to which the offense was committed, the provisions most favorable to the accused have been applied. This provision expresses the recognition of the principle of legality for (substantive) criminal law. Also changes in legislation with regard to the threat of punishment does this apply on the basis of the so-called Scoppola judgment of the ECtHR (ECtHR 17 September 2009, ECLI:CE:ECHR:2009:0917JUD001024903) and the Judgment of the Supreme Court of 12 July 2011 (ECLI:NL:HR:2011:BP6878, NJ 2012/78) the most favorable provision should be applied.

27 Article 83, fourth paragraph, preamble and under a, of the AVG.

28 Only if this would not lead to an appropriate punishment can the amount of the fine be set at a maximum of ten percent of the annual turnover of the legal entity in the previous financial year. Moreover, under the Wbp regime, only a be fined for a data breach after a binding instruction has been given, unless the breach was intentional committed or resulted from serious culpable negligence.

29 Formally, the name change from the Dutch Data Protection Authority to the Dutch Data Protection Authority is the first at the UAVG implemented although the name Personal Data Authority has been used in social circles for some time.

Conclusion on jurisdiction of this legal procedure. This means that, based on the transitional law in the UAVG, the Wbp

this case applies and the AP with regard to the violation of Article 34a, first paragraph, of the Wbp - the
not immediately report a data breach to the AP - is authorized pursuant to Article 48, paragraph 8, of the
UAVG to impose an administrative fine in conjunction with Article 66, second paragraph, of the Wbp.

3.1.4

The foregoing leads to the conclusion that the AP derives its authority from Article 58, second paragraph, opening words
and under i, in conjunction with Article 83, fourth paragraph, sub a of the AVG30 for violation of the
obligation to report referred to in Article 34a, first paragraph, of the Wbp and as included since 25 May 2018 in
Article 33, paragraph 1 and Article 34, paragraph 1 of the GDPR.

3.2

3.2.1

It has been explained above that UBV and UTI use personal data in the sense for the benefit of their services
of the Wbp. In the context of the question of whether the reporting obligation as referred to in Article 34a has been complied
with,
paragraphs 1 and 2 of the Wbp, it is important who can be regarded as the responsible party. The
after all, the controller is the standard addressee.
'Responsible' within the meaning of Article 1, preamble, and under d, of the Wbp, is understood to mean:
Responsible for data processing
Introduction
“the natural person, legal entity or any other body or administrative body that, alone or jointly with
others, determines the purposes and means of the processing of personal data;" 31
It follows from the case law of the Court of Justice of the European Union that the purpose of this provision - die
constitutes the implementation of the concept of 'controller' from Article 2(d) of
Directive 95/46/EC - consists in providing effective and complete protection for data subjects
insurance via a broad definition of the term 'responsible'.32
In this context it is also noted that the AVG in Article 4, paragraph 7, de
defines 'controller' as (materially) equivalent to Directive 95/46/EC and the Wbp.

3.2.2 UBV formal legal responsible

When answering the question of who is responsible, the formal-legal authority plays a role

determine the purpose and means of the data processing play an important role.33 In case of

corporate relationships, as at issue here, the legal entity under whose jurisdiction the

30 This power is enshrined in national law in Article 14, third paragraph, of the UAVG.

31 This description corresponds, where relevant, to the definition of 'controller' in Article 2, under

d, of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of natural

persons in relation to the processing of personal data and on the free movement of such data.

32 CJEU 13 May 2014, Google Spain, SL, C-131/12 9, point 34 (ECLI:EU:C:2014:317) and CJEU 5 June 2018,

Wirtschaftsakademie Schleswig-

Holstein GmbH, C-210/16, paragraph 28 (ECLI:EU:C:2018:388).

33 Parliamentary Papers II 1997/98, 25 892, no. 3, p. 55.

operational data processing takes place as seen by the controller.34 In the

processor agreement of 31 March 2016 (‘Data Processing Agreement’) between UBV and UTI, among others,

UBV is regarded as responsible (‘controller’35) for the processing of (personal) data

that it collects and processes from data subjects outside the United States, including data subjects in

Europe. UTI is then referred to therein as a processor ('processor')36 that for the benefit of UBV

processes personal data.37 The AP is of the opinion that it can be deduced from this that UBV has formally

has legal authority to determine the purpose and means of the data processing and thus

can be regarded as responsible within the meaning of Article 1, preamble, and under d, of the Wbp. This

does not rule out, as explained in more detail below, that in addition to UBV, UTI can also be used as

can be regarded as responsible.

3.2.3 UBV and UTI are jointly responsible

The AP is of the opinion that UBV not alone, but together with UTI aims and means for the processing of personal data. UBV and UTI are therefore jointly responsible to note. Each of the responsible parties, both UTI and UBV, is liable for the entirety of the data processing and compliance with the related obligations.38 Substantiated below the AP takes that position and also includes Uber's view of the AP report. Uber itself considers UBV to be - solely - responsible.39

The controller is the organization that determines the purpose and means of data processing determines. He can do this alone, but also together with others. The AP believes that UBV and UTI are too common regarded as jointly responsible.

Although UBV has formal legal control under the processor agreement, this is not the case by definition decisive for the question of whether UBV is (solely) responsible. As the Article 29-working group - the independent advisory and consultative body of European privacy regulators and currently called the European Data Protection Board - noted in its opinion of 16 February 201040, the provisions in a contract often provide more clarity, but they are not always decisive. The term 'controller' is a functional term, intended to denote responsibilities place where the actual influence lies.41 On the basis of this factual assessment, the AP that UTI and UBV (jointly) make decisions regarding goal setting and means of data processing.

34 Parliamentary Papers II 1997/98, 25 892, no. 3, p. 56.

35 In the English text of Directive 95/46, the term 'controller' is used for controller.

36 In the English text of Directive 95/46, the term 'processor' is used for processor (in Wbp terminology, the processor).

37 See introductory considerations in the data processing agreement (particularly recitals A to D).

38 Parliamentary Papers II 1997/98, 25 892, no. 3, p. 58. This is the third form of responsibility that the legislature for had eyes.

39 Written response Uber dated December 1, 2017, p. 5, answer to question 1 as well as Uber's opinion of 3 July 2018, p. 6.

40 Working Group “Article 29”, Opinion 1/2010 on the concepts of “controller” and “processor”, p. 14.

41 Working Group “Article 29”, Opinion 1/2010 on the concepts of “controller” and “processor”, p. 11 as well

Opinion AG Jääskinen of 25 June 2013 on Google Spain and Google (Case C-131/12), point 83 and AG Bot of 24 October

2017 on

Wirtschaftsakademie Schleswig-Holstein GmbH (Case C-210/16), paragraph 46.

Date

November 6, 2018

Our reference

[CONFIDENTIAL]

With regard to UTI, these are:

- The joint determination of the purpose of the data processing;

- Adoption of the information security policy;

- Decisions on data storage, and

- Developing and offering the Uber app as well as performing updates.

These factors will be explained below.

Joint determination of the purpose of the data processing; uniform privacy policy

UBV and UTI primarily determine the purpose of the processing of the personal data. In the letter dated 7

February 2018 Uber states that the preparation of the privacy statement is a joint effort

of UBV and UTI.42 The introductory paragraph of the privacy statement shows that the

privacy statement applies to both personal data collected in the United States and abroad

are collected. It therefore has a worldwide application range. In the privacy statement, under

'Use of Information' states for what purposes the information can be processed. The by the users

information provided, including personal data, is used for the purpose of:

carry out internal work;

- enable, maintain and improve services;

-

- send messages or enable communication;

- send messages that Uber believes will be of interest to users;

- personalize and improve services.

Back-ups are made of the personal data processed by the Uber group

are stored in its AWS S3 storage in the United States.43 The processing of personal data

for making backups takes place as part of the regular (daily) business process of the

Uber group and can be regarded as such as part of the normal service to

users of the Uber app. The data breach saw personal data in the backups stored in the

(external) AWS S3 storage.44

From the above, the AP concludes that UTI and UBV 'together' have the purpose of processing

determine personal data. The advice of 16 February 2010 of the Article 29 working group states that who

determines the purpose of the processing in any case if becomes responsible for the processing

considered.45 Now that it appears from the foregoing that UTI and UBV jointly pursue the purpose of processing

establish personal data, they are already jointly responsible on that basis.

42 Written response from Uber of 7 February 2018, p. 3. The Uber group had both a privacy statement for users (‘users’) and

for drivers (‘drivers’) and were dated July 15, 2015 with (almost) identical purposes.

43 See further section 4.2.4, p. 18, of the report.

44 See further section 4.3.3, p. 22, of the report.

45 Working Group “Article 29”, Opinion 1/2010 on the concepts of “controller” and “processor”, p. 17.

Date

November 6, 2018

Our reference

[CONFIDENTIAL]

In addition to the purpose, UTI also (partly) determines the means for the processing. It is important to note that notice that even if someone merely determines the means, he can be responsible. The Article 29-

In its aforementioned advice, the working group indicates that only van

responsibility exists when that determination relates to the material aspects of the

resources.46

The Uber group, of which UBV and UTI are part, uses a worldwide

information security policy (Information Security Policy) applicable to all entities of the Uber

concern. This policy, which includes security measures with regard to the protection of

information and (personal) data have been included, has been determined by UTI.47 This concerns, for example for measures with regard to encryption, security procedures in the field of (rights to) access

to information48 and security requirements for Uber's information systems. From the

information security policy also shows that the [CONFIDENTIAL] of UTI is responsible for all

aspects of the security of information, including personal data. It

information security policy states in this regard: “Uber's information security training, guidance, direction,

and authority shall be delegated to the [CONFIDENTIAL].”49 So this is not just about technical or

organizational matters that could be delegated to a processor in themselves.50

The AP is of the opinion that UTI hereby establishes an essential aspect of the resources and this (partly) to it

contributes that UTI together with UBV the purpose of and the means for the processing of personal data

51 Nevertheless, the AP emphasizes that - as explained above - UTI is (partly) the goal of the

processing and can therefore already be jointly responsible with UBV

qualified.

View of Uber and response AP

Uber notes in its opinion on its working method that the controller determines how and why

personal data are processed. That the processor has a certain discretion about details

of the execution of the processing does not make the processor, Uber argues, yet responsible.

46 Working Group “Article 29”, Opinion 1/2010 on the concepts of “controller” and “processor”, p. 17.

47 This can be deduced from the fact that in the Information Security

Policy Version 1.0 of March 9, 2014 on the front page states that “This document is the property of Uber

Technologies, Inc.”. The Information Security Policy Version 0.1 dated August 31, 2016 lists the front page author as "Uber

Inc."

named. In the introduction, the document is introduced as “The Uber Inc (“Uber”or “the company”) Information Security Policy”.

In the subsequent version of the March 2017 information security policy, the front page reads UTI. In the

information security policy that applied at the time of the data breach reported by UBV, it is stated:

“Uber’s information security training, guidance, direction, and authority shall be delegated to the Chief Security Officer (CSO).”

48 For example, the Article 29 working group indicates that the entity that decides, for example, for whom the processed data

must be accessible can be regarded as responsible (recommendation 1/2010 on p. 18).

49 Information Security Policy version 0.1, August 31, 2016, p. 5 (See also AP report dated 1 June 2018, section 4.2.3, p. 18).

50 Cf. advice Article 29 working group 1/2010 on p. 18

51 The Article 29 Working Group notes in its opinion 1/2010 on p. 17 that in some legal systems security measures are

expressly stated

be regarded as an essential feature.

Date

November 6, 2018

Our reference

[CONFIDENTIAL]

Uber hereby refers to the letter of May 14, 2002 from the Dutch Data Protection Authority (CBP).

and the guidelines of the ICO.

The AP does not follow this view and notes that establishing the security policy is not considered "details

of the execution of the processing' can be considered. The AP notes that in the letter from the

CBP from 2002 is explained in general terms that to answer the question who

controller, more weight is given to determining the purposes of the processing
then to determine the details of the processing and that for the demarcation
controller/processor determining the purposes of the processing and control
be decisive. In the AP's opinion, the content of this letter cannot be inferred
that the way in which UTI in particular (actually) operates should lead to the conclusion that UBV and UTI
cannot be considered jointly responsible. On the contrary, as before
noted, UTI also determines the purposes and means of the processing.
In its opinion, Uber also quotes a passage from the guidelines of the ICO, from which, according to Uber
appears that a processor has a certain discretion about details of the implementation of
data processing. The guidelines give an example of a bank that is an IT company
enable data storage.
In response, the AP notes that this example does not warrant the conclusion that UTI is not present in this case
can be regarded as jointly responsible. The role of UTI goes as detailed below
beyond just taking care of the storage as mentioned in the guidelines of the ICO
example. Moreover, being jointly responsible is also determined by handling
of a uniform privacy policy and the determination of the information security policy by UTI as well
the development, offer and updates of the Uber apps and the handling of the
data breach by UTI.
Storage of personal data
The storage of personal data plays an important role in the processing of personal data. Also
with regard to storage, UTI takes important decisions and has a large degree of control.
For example, it is UTI that has entered into an agreement with Amazon for storage for backups. 52
It has been agreed that use will be made of the Amazon storage service AWS S3. In that
connection has also been selected by UTI for the United States as the location for that storage, where
[CONFIDENTIAL].
52 Written response UBV of 12 January 2018, p. 6, answer to question 8.

Date

November 6, 2018

Our reference

[CONFIDENTIAL]

From the above, the AP concludes that UTI is committed to the storage of personal data autonomous from UBV and has had a decisive influence on the way in which the storage - a means of processing personal data - takes place. UTI has (in fact) a big one degree of control over the way in which the processing of personal data takes place. It was more than a mere supporting role and it makes sense when combined with the other facts and circumstances - applying a uniform privacy policy, establishing the information security policy as well as the development, offer and updates of the Uber apps, and the handling of the data breach by UTI - that UTI and UBV are jointly responsible are.

View of Uber and response AP

In its view on the storage, Uber states that it disagrees with the AP's conclusion that UTI is the determining influence of UTI on the location and performance of the data storage as an indicator considered to designate UTI as responsible for data processing. She points out that the processor agreement allows storage by UTI and that UTI as processor also has a sub-processor (in this case Amazon) can enable. In doing so, UTI has ensured that the same obligations apply between UTI and Amazon as between UBV and UTI. According to UTI, this is also a common construction.

In this regard, the AP notes that the circumstance that the storage of personal data by UTI is possible on the basis of the processing agreement and a processor may also use a sub-processor, this does not mean that decisions that UTI has actually made about the storage of personal data - and in combination with the other facts and circumstances mentioned - with it would be irrelevant to the question of whether UBV and UTI can become jointly responsible

marked. The AP is of the opinion that this is not the case. In this regard, the AP emphasizes that UTI has independently taken the aforementioned decisions with regard to the storage without involving UBV in this know. It does not alter the type of decisions and the autonomous occurrence of UTI in combination with the other aforementioned facts and circumstances play a role in the assessment that UBV and UTI are jointly responsible.

Uber app development, offerings and updates

The Uber group offers a service that makes it possible for users to travel via a special purpose developed app (Uber app) to purchase passenger transport. Users are linked to a driver (driver) who can hire customers via another app (Uber Driver app). The special developed mobile applications essentially form the core service of the Uber group.53 UTI54 has developed the Uber app - which serves as the basis for other apps - developed and has licensed UBV to develop the app while Uber app updates are also performed by UTI. 55 With that, UTI contributes to the determination of the purpose and means for the processing of personal data.56 Furthermore, UTI is also the provider of the Uber app in the Apple App store and Google Play Store. That UBV - to Uber in her

53 Cf. introductory recital of the privacy statement for users ("users") and for drivers ("drivers") dated 15 July 2015.

54 And its predecessors.

55 Cf. statement by [CONFIDENTIAL], from UBV on p. 20 of the hearing record.

56 See further section 4.2.6, p. 19 of the AP report.

viewpoint - is responsible for adding new functionalities, does not matter off. Rather, it emphasizes shared responsibility. The circumstance that UTI developer, provider and implementer of updates to the Uber app is still one of the elements that is relevant

for the question whether UBV and UTI can be regarded as jointly responsible. That also applies
with regard to Uber's argument in its view that the provider of the app and the identity of the
developer of the Uber app is irrelevant or not decisive for who is the processor or
is responsible.

Interim conclusion joint responsibility

Based on the aforementioned circumstances, the AP concludes that UBV and UTI jointly
be responsible.

The handling of the data breach by UTI

The AP sees itself confirmed and strengthened in its judgment that UTI and UBV are jointly responsible
due to the autonomous and independent role that UTI has taken in handling the data breach. In that
In this context, the AP notes that the actual decisions about the handling of the data breach - about which UBV
has been informed - independently and solely by it - almost a year after the data breach took place
personnel of UTI have been taken. There are by the [CONFIDENTIAL] of UTI, without UBV herein
knowledge and to give it the opportunity to influence it, specific and important
measures taken. These measures relate to the encryption of files in the AWS S3 buckets and
requiring two-factor authentication for services used by the Uber group and those
be accessible via the internet.57

Uber's position in its view that the independent handling of the data breach by UTI without
involving UBV only demonstrates that UTI is not the obligations under the agreement
fulfilled, the AP does not follow. In doing so, Uber fails to recognize that this actual course of action is precisely the conclusion
of
the AP confirms that UTI makes decisions independently and thus actually has control over the way
on which a data breach is handled.

UTI also has - as Uber indicates in number 2.23 of its opinion - a law firm
[CONFIDENTIAL]requested to engage [CONFIDENTIAL], an external forensic expert. Also
UBV is not known in advance (or immediately afterwards). That it is according to Uber - as it is in its view

states -it was logical that UTI independently conducted an investigation because the incident related to

more US users than Dutch users or that of any other country and UTI the

is responsible for the processing of personal data of users in the United States,

not convincing. According to the AP, it would have been obvious to involve UBV precisely because it is part of the storage

of personal data in the United States also includes personal data collected and

processed from data subjects outside the United States and for this in accordance with the processing agreement

UBV responsible.58

57 More specifically, see section 4.3.4 of the report and the sources referred to in footnotes 101 and 102 originating from

Uber.

58 Uber written response of 7 February 2018, p. 2, answer to question 1.

Date

November 6, 2018

Our reference

[CONFIDENTIAL]

UTI has notified the notifiers of the data breach for the protection of user data59

reward paid. This involves a considerably larger amount than is usually paid.60 UBV

is not involved and not known in the decision-making process. The in this regard with the reporters concluded

agreement has been signed by UTI personnel and on behalf of UTI. UBV was out there.

View of Uber and response AP

In its opinion, Uber notes that the payment to the reporters and the agreement concluded with them

there is no indication that UTI is responsible because it says nothing about determining the purposes

of the processing of user data.

The AP does not follow this argument. UTI's [CONFIDENTIAL] has made it known why

this payment was made: “our primary goal in paying the intruders was to protect our consumers’ data.” It forms

in other words, a means of protecting the (personal) data of the customers of the Uber

concern. That this is done by paying a considerably larger amount than usual and without Involving UBV in this also shows that UTI goes further than a processor can be expected.

In its view, Uber points out that the circumstance that UTI staff - without UBV inform - has dealt with the data breach and taken measures, does not mean that UTI is responsible.

The AP notes that the way in which UTI actually operates and makes decisions where the handling of the data breach is one of the factors relevant to whether UTI as jointly responsible. The role that UTI plays in handling the incident does not stand on its own.

3.2.4 Conclusion of joint responsibility

In view of the above, the AP concludes that UBV and UTI are jointly responsible in the sense of article 1, preamble, and under d, of the Wbp. The AP has taken into account the processor agreement, whereby UBV is designated as responsible. Furthermore, it has been found that UTI together with UBV has determined the purpose of the data processing, UTI itself has established an information security policy, has taken important decisions independently regarding the storage of personal data and has developed and also offers the Uber app and updates for it. The AP's judgment is further strengthened by the independent manner on which UTI has dealt with the data breach in question. Joint responsibility brings with it Please note that each of the responsible parties, i.e. both UTI and UBV, is liable for the entirety of the data processing and compliance with related obligations. Note in this regard the DPA notes that UTI and UBV can also become jointly responsible under the GDPR regime marked.

3.3

59 Uber written response of 7 February 2018, appendix “Testimony Uber (201826).pdf”, p. 5.

60 See further section 4.3.5, p. 25-27, of the AP report.

Violation of obligation to report data breach to AP

18/42

Date

November 6, 2018

Our reference

[CONFIDENTIAL]

Introduction

3.3.1

As appears from subsection 2.1.5, as of 1 January 2016, pursuant to Article 34a, first paragraph, of the Wbp a duty to report data breaches to the AP. Pursuant to this duty to report, the controller must submit to the AP to immediately notify a breach of security, as referred to in Article 13, of the Wbp, which leads to the significant chance of serious adverse consequences or has serious adverse consequences for the protection of personal data. This duty to report contributes to conservation and recovery of public, customer, market, government and regulatory trust in the relevant institution or company when handling personal data.61

3.3.2 The responsible party is the standard addressee

It has been explained with reasons that UBV and UTI are jointly responsible to notice. Both are jointly responsible for compliance with the Wbp for the whole of the processing. This means that both UBV and UTI have an obligation to immediately report a data breach to which Article 34a, first paragraph, of the Wbp related. Uber's position in its view that the obligation to report does not apply to UTI because UTI is not responsible - and therefore none standard addressee - the AP therefore considers incorrect.

3.3.3

Article 34a, first paragraph, of the Wbp refers to a breach of security as referred to in article 13 Wbp (currently article 32 of the AVG). Article 13 concerned a security regulation to which the responsible had to abide by and aimed against 'loss or any form of unlawful

processing of personal data. Unauthorized access is a form of unlawful

processing62 against which the security measures must provide protection. In the present case

as explained below, unauthorized persons from outside the Uber group have access to the

data storage provided by Uber. For example, they could download files that gave them access to,

and could take cognizance of, personal data. Thus, there was a form of illegality

processing.

From October 13, 2016 to November 15, 2016, personal data stored in the AWS S3

storage of UTI accessible to unauthorized persons from outside the Uber group.

In its opinion on page 18, under 3.5, Uber expressly states that it "does not dispute that in that period

there was a breach of security within the meaning of Article 34a Wbp'.63 In this context it is noted that

UTI forensic expert [CONFIDENTIAL] investigated this data breach and her

reported findings.64 [CONFIDENTIAL] was asked to determine to what extent the

Breach of security as referred to in Article 13 of the Wbp

61 Cf. Parliamentary Documents II 2012/13, 33 662, no. 3 Reprint, p. 1 and 3.

62 Cf. Parliamentary Papers II 1997/98, 25 892, no. 3, p. 98.

63 In view of Uber's further argument in its opinion, the AP assumes that Uber has committed the breach of security as

referred to in

Article 13 of the Wbp is not contested.

64 Report [CONFIDENTIAL] of 10 January 2018 with number 138128103.1

unauthorized access to the data stored on the AWS S3 storage:

“[CONFIDENTIAL] was instructed to determine the extent of these outside actors’ access to Uber’s data stored on S3.”

[CONFIDENTIAL] has found that unauthorized users have stolen a total of 16 files from the AWS S3 storage of the Uber group65 and thus had access to and could take note of of the data contained therein. According to the unauthorized persons, they could access the so-called private GitHub repository from Uber using previously leaked usernames and passwords. This eventually allowed them to access the aforementioned AWS S3 files66.

These unauthorized persons have for the first time on October 13, 2016 and for the last time on November 15, 2016 files downloaded from this AWS S3 storage.67 The data breach therefore lasted almost five weeks. During that period, these unauthorized persons could in any case gain access to personal data Uber customers. This included unencrypted personal data such as first name, surname, email address and telephone numbers of Dutch Uber users.68 Uber disputed not, incidentally, that there was a breach of security. This constituted an infringement on the security as referred to in Article 13 of the Wbp, as it applied at the time.

With regard to Dutch Uber users, UBV has made a representative selection of personal data of ten Dutch riders and drivers as they are in the back-ups of the databases downloaded by the unauthorized. This shows that, among other things, first name, last name, e-mail address and telephone numbers of Dutch Uber users are present in the downloaded database backup were.69

3.3.4

Pursuant to Article 34a, first paragraph, of the Wbp, there is first a notifiable breach of the security if that breach “leads to the significant likelihood of serious adverse consequences or serious adverse has consequences for the protection of personal data”.

Because in this case unauthorized people have downloaded files from Uber on its AWS S3 storage and thus had access to and could take cognizance of the personal data contained therein Uber customers were involved in unlawful processing and have adverse consequences for the protection of personal data has actually manifested itself. That is why it is judged of the AP has serious adverse consequences. This is in the words of the memorandum of

Infringement has a (considerable chance of) serious adverse consequences

65 Cf. the findings of [CONFIDENTIAL]as recorded in her report on p. 4 and 5. In the letter of 22 October 2018 additional addendum to the report of January 10, 2018, following an analysis of additional logs, which were subsequently reinforced to [CONFIDENTIAL] by Uber, established by [CONFIDENTIAL] that the unauthorized persons outside the 16 files described in the original report dated January 10, 2018 no other files were downloaded.

66 Cf. email conversation on November 15, 2016 from an Uber employee and the reporter (Appendix 3 to Uber's letter of 11 December 2017) as well as paragraph 3.9 of Uber's opinion.

67 Appendix b, table 3, p. 11 and 12 of the report of [CONFIDENTIAL].

68 Cf. Letter UBV 11 December 2017, appendix 2, letter UBV 12 January 2018 (response to question 17) and the [CONFIDENTIAL] report, p. 7 -9.

69 Cf. Letter UBV 11 December 2017, appendix 2, letter UBV 12 January 2018 (response to question 17) and the [CONFIDENTIAL] report, p. 7 -9.

explanation to a 'successful hacker attack', which in itself is an important indication of that there is a data breach that must be reported.70

With regard to the scope of the personal data involved in the data breach, the AP notes that forensic expert [CONFIDENTIAL] found that 57,383,315 Uber users were involved in the data breach involved, of which 25,606,182 American and 31,777,133 non-American.71 It also appears from information from Uber that approximately 174,00072 Dutch Uber users have been affected by the data breach.

With regard to the personal data involved in the data breach, the AP also notes that it concerns - as can be are taken from the research carried out by [CONFIDENTIAL] - 31 species

personal data, as shown in the section 'facts and process'.

The size of the personal data involved in the data breach, the large number of different types

personal data, the type of personal data (names, e-mail addresses and telephone numbers) as well as the

fact that it concerns personal data of customers of one specific – globally operating –

company, make the personal data extra attractive, for example to be resold73

for activities such as '(spear) phishing'74, unwanted advertising (spam) and/or unwanted

telephone canvassing.75

Apart from the fact that unauthorized persons have gained access to Uber's storage and therefore already

it can be argued that there is a (considerable chance of) serious adverse consequences, as referred to in

Article 34a, first paragraph, of the Wbp, this is all the more the case, at least in view of the

the scope of the personal data involved, the type of personal data and the fact that it originates

goods of customers of one company, which is moreover active worldwide. As a result was Uber

required by law to report the data breach. Uber's argument that of serious adverse consequences,

at least the considerable chance of this would not exist, the AP therefore considers incorrect.

Merely by way of illustration, the AP notes the following in this regard. If Uber actually meant it

that it should not have reported the data breach, the AP is surprised that UTI has nevertheless decided to

to 'reward' the reporters of the data breach with an amount that was substantially higher than what is normal

spoken, and has stipulated secrecy with them regarding the data leak.76 This implies

70 Cf. Parliamentary Documents II 2012/13, 33 662, no. 3 Reprint, p. 7.

71 Report [CONFIDENTIAL], p. 7-9.

72 Cf. annex 4 to Uber's letter dated 1 December 2017 (answer to question 5).

73 For example on the black market via the 'dark web'.

74 Phishing is a form of internet fraud in which someone receives false e-mails that try to direct them to a fake website.

to lure. cf. https://www.rijksoverheid.nl/onderwerpen/cybercrime/question-and-answer/phishing. One form of phishing is spear

fishing. The personal data (name, e-mail address, telephone number) of the victim are used to provide him with a

to give a sense of confidence. An email arrives that appears to be from a reliable source, but in

in reality, it leads the user to a counterfeit website, which is, for example, full of malware. Such a targeted attack is common more successful than a general phishing campaign.

75 Cf. section 4.2.2, p. 27-28 of the policy rules 'The obligation to report data leaks in the Personal Data Protection Act (Wbp)' of 8

December 2015 (Stcrt. 2015, no. 46128). See also:

https://autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-publishes-policies-rules-

duty to report data leaks

76 In this context, reference is made to what has been considered in this decision in the case of seriously culpable negligence.

according to the AP, it is precisely that Uber apparently considers the data leak to be particularly serious and also serious had adverse consequences for the protection of personal data, or at least had a considerable chance of doing so existed. The notifier of the data breach has also explicitly pointed out the risks to Uber, although he may have also had other intentions77: “Let me tell you this looks bad. I suggest you speak with employees on re-using passwords. My team was able to access a lot of internal information. [CONFIDENTIAL]"

The impact and seriousness of the data breach and thus supporting the AP's conclusion that there is of (the significant chance of) serious adverse consequences, can also be deduced from the fact that the [CONFIDENTIAL] of UTI before a subcommittee of the United States Senate.

has defended the higher than normal amount paid to the reporting persons and has stated that this is done with a view to protecting the personal data of Uber customers.78 In addition,

the CEO of Uber publicly publicized the data breach through a notice to her website.79 It has also emerged from various public sources, including the Uber website, that Uber in connection with the concealment of this data breach, a settlement worth USD 148 million was recently reached

has quarreled with the authorities in the United States.80 The AP also follows Uber against this background

not in its statement that of serious consequences for the protection of personal data, or the

considerable chance of that, would not be the case, and Uber only made the notification "voluntarily and on its own."

movement' and 'in the context of transparency'.

Other parts of Uber's view and AP's response

That the unauthorized persons have - to date - not further distributed, resold or

otherwise processed does not mean, according to the AP, that, as Uber argues in its opinion,

there was therefore no question of (a significant chance of) serious adverse consequences for the

protection of personal data. The AP refers to what has been considered above in this section

about the (considerable chance of) serious adverse consequences. Also the ones posited by Uber in this regard

statement in its view that there is no question of personal data of a sensitive nature, means according to it

the AP does not rule that a data breach such as the present one does not have to be reported. Other than

Uber believes that cannot be deduced from the policies either. The policies state: (…) A

A factor that plays a role in this is the nature of the leaked personal data. If there is personal data of a sensitive nature

leaked, then a notification is generally necessary. (…).81In short, it is one of the relevant factors

answering the question of whether a data breach is notifiable. However, according to the AP, that does not mean that

in the event that personal data has been leaked that is not sensitive, the data leak is therefore always subject to the reporting

obligation

would have been changed. Also other factors such as the amount of leaked personal data per person or

77 See e-mail exchange on 14, 15 and 16 November 2016 between the reporter and Uber employees (Appendix 3 to the letter

from Uber dated 11

added December 2017).

78 See appendix to Uber's letter of 7 February 2018.

79 Cf. under 4.26 of the Uber opinion, p. 30.

80 See for example: https://www.uber.com/newsroom/2016-data-breach-settlement/, https://www.reuters.com/article/us-uber-

databreach/uber-settles-for-148-million-with-50-us-states-over-2016-data-breach-idUSKCN1M62AJ,

https://nos.nl/artikel/2252243-

uber-settles-for-148-million-dollar-after-silence-data-leak.html, https://www.iowaattorneygeneral.gov/newsroom/uber-hackers-

data-breach-miller-attorneys/ and

https://oag.ca.gov/news/press-releases/california-attorney-general-becerra-san-francisco-district-

attorney-gasc%C3%B3n

81 Cf. Policy rules 'Notification obligation data breaches in the Personal Data Protection Act (Wbp)', p. 2.

Date

November 6, 2018

Our reference

[CONFIDENTIAL]

the number of data subjects whose personal data has been leaked may lead to the data breach

report. This is also apparent from the policy rules.82 The above also applies to Uber's statement in her

view that the data breach was resolved on November 15, 2016, the unauthorized persons were after a reward

and there was no indication of misuse or likelihood of misuse of personal data. Also this one

circumstances, whatever the case may be, do not entail that the present data breach does not

was required to report.

3.3.5 Data breach not reported immediately

If there is a data breach that is subject to a notification requirement, Article 34a, first paragraph, of the Wbp obliges the

controller to inform the supervisor of this 'immediately'. What in a concrete

case should be regarded as 'promptly' depends on the circumstances of the case. Rational is that

the controller must be given some time to investigate the breach. The legislator

has left it to the supervisor to further define the term 'immediately'.83 The AP has this

done in the aforementioned policy rules 'Notification obligation data breaches in the Personal Data Protection Act (Wbp)'

of 8 December 2015.84 The notification of the data leak must - according to paragraph 6 of the policy rules -

to the AP without undue delay, and if possible no later than 72 hours after discovery

done. The main rule is therefore that the notification must be made without undue delay, whereby 72 hours in principle applies as the ultimate limit. In this context, it should also be noted that a provisional notification can be done.85 In practice, this will not easily give rise to not complying with the stipulated period of 72 hours to report a data breach.

As stated earlier, UTI and UBV are regarded by the AP as jointly responsible. On Monday, November 14, 2016 UTI has been made aware of a vulnerability in her data security. After all, on that date the then [CONFIDENTIAL]from UTI received an e-mail mail message from a person86 who informed the [CONFIDENTIAL] that he had a major vulnerability had discovered the data security of the Uber group.87 On November 15, 2016, documents containing the relevant personal data were downloaded therein and could be viewed.88 The unauthorized in the email correspondence to Uber on "(…) ALL INTERNAL data was able to be downloaded and seen (…)" and "(…)[CONFIDENTIAL] (…)". On November 15, 2016, the [CONFIDENTIAL] of UTI ordered to change access codes to Uber's AWS S3 storage.89 Based on the information regarding the infringement which UTI therefore already had at its disposal on 15 November 2016, UTI was forced to to take measures.

82 Ditto.

83 Cf. Parliamentary Papers II 2013/14, 33 662, no. 6, p. 16.

84 Stct. 2015, 46128, p. 14-15.

85 For example, because it is not yet clear what happened and which personal data are involved. If necessary, the notification can then be made be added or withdrawn. cf. section 6, p. 31 of the policy rules 'Notification obligation data breaches in the Protection Act personal data (Wbp).

86 This person used a pseudonymous e-mail address.

87 This e-mail is attached as appendix 3 to Uber's letter of 11 December 2017.

88 Appendix b, table 3, p. 11 and 12 of the report of [CONFIDENTIAL].

89 Cf. email conversation on November 15, 2016 (more specifically, the email to the reporter dated November 15, 2016 at 9:29

AM), which as

appendix 3 to the letter from Uber dated December 11, 2017 is attached.

23/42

Date

November 6, 2018

Our reference

[CONFIDENTIAL]

In view of the above, the AP is of the opinion that UTI had already reasonably reported on November 15, 2016

can and must make of the data breach, because a report after that moment in view of the above

In the opinion of the AP, the circumstances mentioned can be qualified as 'unnecessary'

delay" as referred to in the policy rules. But in any case, the report had to be made within 72 hours after 14

November 2016 - the day Uber was notified of the data breach - should take place. This had

also reasonably have to be done if the exact size of the data breach is not yet known at that time

known or could not yet be assessed. As mentioned, a provisional notification could also be made

done.

On November 21, 2017, UBV reported the data breach to the AP by means of the information on the website of the

AP provided web form. The period for reporting the data breach starts according to this

aforementioned policies:

"to run the moment you, or a processor you have engaged, becomes aware of an incident

that may fall under the obligation to report data breaches."90

UTI and UBV are jointly responsible and therefore the duty rested on both UTI and UBV separately

to report the data breach no later than 72 hours after UTI was notified of it on November 14, 2016

to report to the AP. The data breach was first reported on November 21, 2017, making it 371

days after its discovery, which exceeds the prescribed period of 72 hours

exceeded. An immediate notification as referred to in Article 34a, first paragraph, of the Wbp is therefore

no way. The AP does note that, now that UBV has reported the data breach to the AP on November 21, 2017,

reported, the AP considers this report to have been made also on behalf of UTI. UTI therefore does not need the notification (again) to do.

Apart from that, the AP notes that the period for reporting on the basis of the policy rules is now (partly) extended determined by the time at which the processor becomes aware of the incident - and insofar as UTI in this context should be classified as a processor - Uber cannot hide behind the circumstance that UTI as a processor has merely failed to fulfill its obligations under private law towards UBV, as it puts forward in its opinion.

Completely superfluous, the AP also notes that even in the case of UBV as (only) should be regarded as responsible, or if UBV is there – as joint person responsible with UTI – can justifiably claim that they are only at a later time by UTI has been informed of the data breach, the notification on November 21, 2017 by UBV to the AP is still has not been done 'immediately' after being informed by UBV. UBV is in the person of the [CONFIDENTIAL] after all, on October 25, 2017, became aware of what Uber calls in its opinion an “IT security incident in 2016, that it was being investigated, and that it could potentially create a media cycle.”91 In the judgment of the AP, UBV cannot justifiably claim ignorance, which consists in that the

90 Cf. section 6, p. 31 of the policy rules 'The obligation to report data leaks in the Personal Data Protection Act (Wbp)'.

91 Annex 1 to Uber's written opinion dated 3 July 2018.

[CONFIDENTIAL] from UBV had no “knowledge of the scope of the incident, or if personal data was involved”.92 With the information that was known to [CONFIDENTIAL] of UBV on October 25, 2017 - an IT security incident that can cause potential media attention - in the opinion of the AP reasonably in his position to ask critical questions in order to find out whether this was the case

a data breach, whether personal data were involved and what the relevance of the 'IT security incident'
was for UBV. And even if it must be assumed that UBV will first enter November 10, 2017
would have been notified of the data leak, as Uber argues,93 there is still a broad
exceeding the prescribed period of 72 hours and is not an immediate notification either
talk.94

As explained above, the importance of an immediate report lies, among other things, in the
maintain and restore public, customer and regulatory trust in Uber. A
immediate notification enables the AP to form its own view of the facts in a timely manner, to form an opinion
can provide information about the measures taken and, under certain circumstances, confidentially with the
can consult with the responsible party and intervene if necessary.95 Because in this case the
prescribed period of 72 hours has been amply exceeded and therefore of an immediate notification
of the data leak can by no means be spoken of, there is a situation in which that confidence is in high
mate is ashamed. In this context, it is emphasized once again that a data breach is also possible subject to conditions
be reported and can be supplemented or withdrawn if necessary.

View of Uber and response AP

The explanation given by Uber for not reporting to the AP within the 72-hour period of the
data breach has been regarded in the investigation report as insufficiently motivated. Uber has indicated that
was not reported in time, but that it cannot explain why this was not done.96 Uber's position in
her view in which she indicates that UBV, after being informed by UTI of the data breach
has reported the data breach to the AP within an 'adequate' period of 21 November 2017 (and via its
authorized representative on November 20 of the intention to report to the AP) is convincing
the AP does not. As noted, (also) UTI, as (jointly) responsible on November 15, 2016,
in any event no later than 72 hours after UTI became aware of the data breach on November 14, 2016
stated, can and must report the data breach.

In its opinion, Uber also states that the notification form was not made for foreign users
companies and is specifically aimed at Dutch companies. The AP notes in this regard

that it cannot be concluded from this that this would dismiss UTI, as joint controller

of its obligation to report to the AP or that this would be an impediment to (immediately) report the data breach.

UTI could have contacted AP about this. The AP remarks superfluously that

92 Ditto.

93 According to section 5.26, p. 37 of Uber's view in any non-disputable as the date UBV by UTI

has been notified of the data breach.

94 An immediate report, i.e. within 72 hours and, if necessary, conditionally, would have been the obvious choice then

because the data breach

already occurred in 2016.

95 Cf. Parliamentary Documents II 2012/13, 33 662, no. 3 Reprint, p. 4.

96 Cf. section 5.3.3. p. 38 -39, of the research report.

the website of the AP also has an English version that points to the possibility with the AP

to get in touch. Moreover, UTI could have used UBV as a point of contact or one

authorized representative in the Netherlands.

3.3.6 Conclusion

From the above, the AP concludes that UBV and UTI, as (jointly) responsible on 15

November 2016, at least within 72 hours after UTI was notified on November 14, 2016

of the data breach pursuant to Article 34a, first paragraph, of the Wbp, the data breach was/were obliged to

report to the AP. However, the notification to the AP only took place on November 21, 2017 and was

not immediately as referred to in that paragraph. In view of this, there is a violation of Article

34a, first paragraph, of the Wbp, whereby UBV and UTI are both offenders. As far as it should be

assumed that - in the interpretation of Uber - only UBV is responsible and UTI processor,

does this assumption not lead to a different conclusion, now that the period of 72 hours is based on the policy rules

runs from the time the processor (UTI in this case) becomes aware of the incident, te

know November 14, 2016.

3.4

Violation of reporting obligation to the person concerned

Introduction

Infringement is likely to have an adverse impact on privacy

3.4.1

As can be seen from subsection 2.1.5, as of 1 January 2016, pursuant to Article 34a, second paragraph, of the Wbp

a duty to report data breaches to those involved. Pursuant to this obligation to report, the controller must

notify the data subject without undue delay of a security breach if the breach is likely

will have unfavorable consequences for his privacy. Both UBV and UTI is, as jointly

responsible, standard addressee thereof. In this context, the AP refers for the sake of brevity to what is stated in

has already been considered above about the violation of the obligation to report to the AP. The same applies to

regarding the security breach.

3.4.2

Pursuant to Article 34a, second paragraph, of the Wbp, a notifiable breach is defined as the breach

is likely to have unfavorable consequences for the privacy of the data subject(s) who use it

concerns. Because in this case unauthorized files of Uber from its AWS S3 storage

downloaded and thus had access to and could take cognizance of the contained therein

personal data of Uber customers, in the opinion of the AP, there are unfavorable consequences for the

privacy of the data subjects whose personal data it concerned. The AP notes with respect

of the scope of the concept of personal privacy, which becomes personal data

protected as part of privacy within the meaning of Article 10 of the Constitution and

as part of the right to respect for private life within the meaning of Article 8 of the ECHR.97 Everyone

has the right to have his personal data processed in a lawful manner, in order to prevent

that he suffers from this.

97 Parliamentary Papers 2017/18, 34 851, no. 3, p. 7.

Date

November 6, 2018

Our reference

[CONFIDENTIAL]

In addition to the fact that unauthorized persons had access to Uber's storage - and therefore to the

stored personal data of Uber customers – makes the scope of the data breach involved

personal data98, the type of personal data (names, e-mail addresses and telephone numbers) as well

the fact that it concerns personal data of customers of one specific - globally operating -

company that there is even more (probable) adverse consequences. Through this combination of

factors, the dataset becomes extra attractive, for example to be resold99 for the benefit of

activities such as (spear) phishing100, unwanted advertising (spam) and/or unwanted telephone canvassing.

When in mid-November 2016 Uber became aware of the data breach and the personal data that

involved, there was sufficient reason to report to those involved because of

foreseeable adverse consequences, such as the risk of (spear) phising, for example. At that point it was

a real risk and could not reasonably be excluded.

Based on the foregoing, the AP concludes that Uber in this case, pursuant to Article 34a, second paragraph,

Wbp, was obliged to report the data breach to the data subjects concerned. In this regard, the

The AP also notes that it has not been stated or proven that a situation as referred to in Article 43 occurs

Wbp and on the basis of which the controller does not comply with the notification obligation from Article 34a, second

paragraph, Wbp

application can.

3.4.3 Data breach not reported (immediately).

The AP establishes that the data leak was not reported to the parties involved and therefore there was also no an immediate notification, as required by Article 34a, second paragraph, of the Wbp. What in a specific case to be regarded as prompt depends on the circumstances of the case. In the several times the aforementioned policy rules on data leaks, the AP indicates that reporting immediately means that after the discovering the data breach, some time may be taken for further investigation so that those affected can be informed in a proper and careful manner by the responsible party. From the policy rules also shows that, just as with the notification to the AP, it is possible to opt for the to inform those involved in the first instance on the basis of the information available at that time so that those concerned can take measures in advance. One measure can already mean that stakeholders to be extra careful. The information can then be supplemented later if necessary.101 Against this background, and with reference to what has been noted about this in this decision with regard to the violation of the obligation to report to the AP, it is noted that Uber was informed of the data breach on November 14, 2016 has been set. The AP is of the opinion that Uber will be calculated from November 14, 2016 at the latest within 72 hours, and in line

98 It has already been indicated above in this decision that the data of 57,383,315 Uber was violated with regard to the obligation to report to the AP.
users, of which 25,606,182 are US and 31,777,133 are non-US. As far as Dutch Uber users are concerned to about 174,000 affected.

99 For example on the black market via the 'dark web'.

100 Phishing is a form of internet fraud in which someone receives fake e-mails that try to direct them to a fake website. to lure. cf. https://www.rijksoverheid.nl/onderwerpen/cybercrime/question-and-answer/phishing. One form of phishing is spear phishing. The personal data (name, e-mail address, telephone number) of the victim are used to provide him with a to give a sense of confidence. An email arrives that appears to be from a reliable source, but in in reality, it leads the user to a counterfeit website, which is, for example, full of malware. One such targeted attack is often more successful than a general phishing campaign.

101 See p. 45 of the data breach policies.

inform the parties involved of what the AP has considered with regard to the obligation to report to the AP should and could have made of the data breach. That didn't happen.

3.4.4 How should the data breach be reported to data subjects?

Pursuant to Article 34a, paragraph 5, of the Wbp, the notification to the data subject is made in such a way manner done that, taking into account the nature of the infringement, the detected and the actual consequences for the processing of personal data, the circle of data subjects and the costs of implementation, a proper and careful provision of information is guaranteed.

Reporting a data breach to those involved should - as follows from the policy rules on data breaches and the legal history102 - to be done on an individual basis, such as in a personal e-mail. By far the most In some cases, the controller will have and will be able to provide contact details of the data subjects data subjects are also informed individually. In the case of more extensive incidents, a combination of general and individual information provision are appropriate, such as a notice on the company website and an individual email to affected customers. The main thing is that so much potentially involved parties are reached and informed about the measures to be taken by him or her measures to limit the consequences for privacy as much as possible. With just one as reported in the media, that goal has not been achieved.103 In the opinion of the AP, in view of the for Uber available contact details make it possible to approach affected Uber customers individually and reporting in a press release alone was not sufficient.

3.4.5

In its view, Uber states that the data breach did not have to be reported to those involved because there was various technical and organizational security measures have been taken. Regarding that

the AP notes that the security measures taken by Uber were aimed at preventing the data leak close and prevent recurrence. However, this does not mean that it should be concluded that during the period of the infringement there was no situation that made the infringement likely will have adverse consequences. As explained above, the AP is of the opinion that there is a infringement likely to have adverse consequences. Also justify the hit by Uber measures do not invoke Article 34a, paragraph 6, of the Wbp on the basis of which a notification to person concerned can be omitted. Lots of personal data - including names, email addresses and telephone numbers - were after all unprotected (unencrypted) and accessible to and in the possession of unauthorized persons. The measures to which Uber refers were, as said, afterwards taken to close the leak and prevent recurrence.

Uber also indicates that it was unlikely that the data breach would have adverse consequences because it is not about sensitive data.

View of Uber and response AP

102 Cf. p. 43 of the policy rules on data leaks and Parliamentary Papers I, 2014/15, 33 662, no. C, p. 15.

103 Parliamentary Papers I, 2014/15, 33 662, no. C, p. 15.

In the event that personal data of a sensitive nature has been leaked, it must be assumed that the data breach must be reported not only to the AP, but also to those involved.104 It is with others words a very important indication that a report must be made to data subjects. Based upon of the policy rules shows that in all other cases the controller is responsible on the basis of the circumstances of the case will have to be weighed up. The circumstance that a data breach is not concerns sensitive data, this does not mean that a notification to data subjects can therefore be omitted

to stay. In this case, there were sufficient reasons for which Uber was held accountable for the data breach
inform those involved.
Uber further argues in its view that there is no evidence that more than two individuals during one
had access to the relevant personal data for a short period of time, which made Uber login data unusable
created and implemented two-factor authentication. According to Uber, everything indicates that the
unauthorized persons have deleted the downloaded files without sharing them with others. Uber has
confidentiality agreements signed with the unauthorized persons and knows their identity. That determined
personal data were available for a short period of time to two individuals, according to Uber, it does not matter
likely that the conscious personal data (names, e-mail addresses, telephone numbers) for spam
whether phising are used, quite apart from whether this can be seen as a breach of the
personal living ambiance.
The AP does not follow Uber in its argument. That there are indications that the unauthorized persons have the files
removed, they have signed a confidentiality agreement and have disclosed their identity, and
according to Uber, it is unlikely that the personal data in question is for spam or phising
used, does not alter the fact that the personal data were accessible to unauthorized persons and that this, such as
previously considered, given the scope and type of personal data and the fact that it concerned customers
of one company represented a significant risk of further dissemination. By the way, this also applies
It cannot be ruled out at the moment that the data in question is not yet available somewhere - outside of Uber
are. The data breach lasted for five weeks. During that period, the unauthorized
access to the relevant personal data without Uber having any influence. That has, like
set out above, entails risks. That was the opinion of the AP
sufficient reason to conclude that the data breach had been reported pursuant to Article 34a, second paragraph, Wbp
should be made available to those involved.
Finally, in its view, Uber states that it derives from the passage of time and the lack of any indication of
the AP regarding notification to data subjects - the AP has since the notification of the data breach to the AP
November 2017 Uber not obliged to report the data breach to the person concerned - was allowed to open

that the AP also believes that it is unlikely that the data breach could have adverse consequences for the data subjects.

The AP does not follow Uber in its argument. To this end, the AP notes first of all that it is up to UTI and UBV as is responsible for assessing whether a data breach should be reported to those involved and not to the data breach

104 Cf. p. 39 of the data breach policy.

Date

November 6, 2018

Our reference

[CONFIDENTIAL]

Seriously culpable negligence

AP.105 That assessment must be made at the time the data breach was known to Uber. That was already on November 14, 2016. As explained above, there was sufficient reason to do so data subjects to report the data breach. In hindsight, this has not yet been proven unfavorable consequences as a result of, for example, phishing activities, in the opinion of the AP not different. The assessment of whether the data breach has or will have serious consequences for the protection of personal data must be created at the time of the data breach.

3.4.6 Conclusion

From the above, the AP concludes that UBV and UTI, as jointly responsible parties involved wrongly and contrary to Article 34a, second paragraph, of the Wbp of the data breach. Therefore, there is a violation of 34a, second paragraph, of the Wbp, whereby UBV and UTI are both offenders.

3.5

3.5.1

For this, the AP has concluded that UBV and UTI are jointly responsible in the sense of Article 1, preamble, and under d, of the Wbp, as a result of which UBV and UTI are both standard addressees of the

obligation pursuant to Article 34a, first and second paragraph, of the Wbp. Failure to timely reporting the data breach to the AP and timely notification of those involved is, in the opinion of the AP the result of seriously culpable negligence. The AP explains its position below. To that she will first of all explaining the legal framework and outlining what knowledge a standard addressee considers it to be becomes to have. Subsequently, the AP will review the Uber group's knowledge of the seriousness of the data breach judge. Subsequently, the AP will indicate facts and circumstances that, in the opinion of the AP, make that the failure to report the data breach to the AP in a timely manner and to notify it in a timely manner involved is the result of seriously culpable negligence.

3.5.2 Legal framework

At the time of the violation, Article 66, third and fourth paragraph, of the Wbp read, insofar as relevant, as follows:

Introduction

"(…)

3. The Board will not impose an administrative fine for violation of the provisions of or pursuant to the Article 66, second paragraph, said Articles, then after it has issued a binding instruction. The College can set a time limit within which the instruction must be complied with.

The third paragraph does not apply if the violation was committed intentionally or is the result of serious culpable negligence.

4.

(…)"

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

105 Cf. p. 39 of the data breach policy

Date

November 6, 2018

is the result of gross, significantly negligent, negligent or injudicious acts.”106 In this context
it is noted that “acting” as referred to above also includes an omission.107

Both in the parliamentary history and in the Policy Rules on the obligation to report data breaches from 2015
examples of data leaks that must be reported to the AP. By way of illustration, below
more mentioned:

-

- on the website of a telephone company, customers can log in and enter their financial data and
a company suffers a hack in which customer data and passwords have been stolen;
view call details. A third party has gained access to the database with login names and
associated scrambled (blacked out) passwords. However, it is possible that certain
passwords can be retrieved. 108

The Policy Rules on the obligation to report data breaches also address the question of when a data breach is required
are reported to the AP. According to Article 34a, first paragraph, of the Wbp, this must be done “immediately”.
The AP has specified the term “immediately” in the Policy Rules on the Data Leak Reporting Obligation.
For the sake of completeness, the AP quotes the relevant passage in full.

“6. When do I have to report the data breach to the Dutch Data Protection Authority?

You must immediately report the data breach to the Dutch Data Protection Authority (article 34a, first paragraph, Wbp).
Reporting without delay means that you are allowed to take some time after discovering a possible data breach
further investigation in order to avoid an unnecessary report.

What qualifies as 'promptly' in a specific case will depend on the circumstances of
the case. Below you will find the principles that the Dutch Data Protection Authority has in mind
uses supervisory and enforcement powers.

The period for reporting the data breach starts when you or a processor you have
becomes aware of an incident that may fall under the data breach notification obligation.

Without undue delay, and if possible no later than 72 hours after discovery, report to the

Dutch Data Protection Authority, unless your investigation has already shown that the incident has occurred at that time does not fall under the obligation to report data breaches. If you report the incident later than 72 hours after discovery to the supervisor, you can, if asked, motivate why you made the report later.

You may not have full insight into what happened and for what reason 72 hours after the discovery of the incident personal data it concerns. In that case, you make the report based on the information you have at that time features. If necessary, you can supplement or withdraw the notification afterwards.

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

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

108 Parliamentary Papers II 2014/15, 33662, no. 11, p. 11, Parliamentary Papers I 2014/15, 33662, no. C, p. 24 and Policy rules on the obligation to report data breaches,

stcrt. 2015, 46128, p. 14-15.

Date

November 6, 2018

Our reference

[CONFIDENTIAL]

To be able to report data leaks in a timely manner, you will have to make good agreements with the processors you may use so that they inform you in a timely and adequate manner about all relevant incidents."

The AP takes a position with regard to the knowledge that a standard addressee (UBV and UTI jointly) has of the applicable laws and regulations is deemed to have the position that is based on te

market parties bear their own responsibility to comply with the law.109

The AP has also provided ample information to market parties about the applicable laws and regulations, so that it can be assumed that Uber was also aware of this. In addition, there is extensive attention in the media spent on the obligation to report data breaches.

From the legal framework set out above in conjunction with the explanatory notes and the Policy Rules

obligation to report data breaches, which Uber could have become aware of before the data breach, follows to the
the AP's opinion is sufficiently clear that Uber attributed the data breach to both the data subjects and the AP
must report and that this without delay, but in any case no later than 72 hours after the discovery on 14
should have taken place in November 2016. Moreover, the report to the AP could have been conditional
be made, in the sense that the notification could be supplemented afterwards. That possibility
is expressly provided in the policy rule.
If doubt had arisen about the scope of the commandment, then, also according to settled case law, te
apply that may be expected of a professional and multinational market party such as Uber
that it informs itself properly or is informed about the restrictions on its conduct
subject, so that she could have tailored her behavior to the scope of that from the outset
commandment.110

3.5.3 Science of the Uber group about (the seriousness of) the data breach

In the opinion of the AP, UTI's management was aware of the seriousness of the data breach. like that
is firstly apparent from the speed with which UTI has agreed to pay an amount to the
reporters of the data breach. Furthermore, the amount paid to the notifiers is substantially higher than usual.
In addition, this is apparent from the additional agreements that are concluded with
the notifiers are closed with the intention of keeping the data breach secret. The AP explains this as follows.

3.5.3.1 Payment approval speed

On Monday, November 14, 2016, UTI was made aware of a vulnerability in her
data security. After all, on that date the then [CONFIDENTIAL]from UTI received an e-mail
mail message from a person who informed the [CONFIDENTIAL] that he found a major vulnerability in the
data security of the Uber group.111 On the same day, the reporter informed UTI
made it known that he and his team received “high compensation” for signaling the data breach to UTI
to expect.

109 Cf. CBb 25 June 2013, ECLI:NL:CBB:2013:4, r.o. 2.3, CBb 25 January 2017, ECLI:NL:CBB:2017:14, r.o. 5.2, CBb March
8, 2017,

ECLI:NL:CBB:2017:91, r.o. 6.

110 Cf. CBb 22 February 2012, ECLI:NL:CBB:2012:BV6713, r.o. 4.3, CBb 19 September 2016, ECLI:NL:CBB:2016:290, r.o. 8.6., CBb 19

September 2016, ECLI:NL:CBB:2016:372, r.o. 6.3.

111 This e-mail is attached as appendix 3 to Uber's letter dated 11 December 2017.

Date

November 6, 2018

Our reference

[CONFIDENTIAL]

On Tuesday, November 15, 2016, the reporter will report to [CONFIDENTIAL], who will terminate contact with the reporter maintained, knowing: “I am happy that you guys finally found the issue, it was the aws keys that have been leaked, ALL INTERNAL data was able to be downloaded and seen, your security steps are very poorly done, the lack of negligence and care here is zero to none. Your employees are careless and don't care about security. Me and my team found that your team lacks 2 step authenticator on github.”

The [CONFIDENTIAL] asked on November 15, 2016 about the seriousness of the data breach: "I'm trying to get some idea on payout amount - can you provide a full list of things you were able to access? That will help me understand impact and then I can pitch an award amount to management.”

In response, the reporter says: “Let me tell you this looks bad. I suggest you speak with employees on re-using passwords. My team was able to access a lot of internal information. [CONFIDENTIAL]."

Already on Friday 18 and Monday 21 November 2016, agreements were signed by the [CONFIDENTIAL] of UTI and two individuals. These agreements regulate the payment of – in total – $100,000 for reporting the data breach to UTI.112

UTI's [CONFIDENTIAL] filed a copy of the agreement with UTI on Tuesday, November 22, 2016 forwarded to the notifiers.113 The UTI employee confirmed this to the notifiers when asked that the payment of the bug bounty could be made in bitcoin.114

On Friday, December 9, 2016, an amount of 65,508 BTC was sent to the bitcoin address of the reporter, who confirmed on the same day that he had received the bitcoins.115 On Thursday, December 15, 2016, once sent an amount of 64.02 BTC to the same address.

E-mail exchanges also show that on December 23, 2016, UTI's [CONFIDENTIAL] was informed of the progress of measures taken in response to the data breach.116

3.5.3.2 Above-average remuneration

UTI paid the reporters a $100,000 reward for reporting the data breach. This amount is paid through Hacker One's bug bounty program. This is a substantially higher amount than usual for reporting a vulnerability is paid by the Uber group. Unlike Uber sets in its view, this is equally a strong indication in the AP's opinion that UTI was aware of the seriousness of the data breach. A different explanation for paying a significantly higher amount than usual, Uber has not given. Despite the payment being made through HackerOne, Uber has communicated that the payment was not made as part of the normal Bug Bounty

112 Annex 3 to Uber's letter of 11 December 2017, as well as the annex to Uber's additional written response of 21 February 2018.

113 This e-mail is attached to Uber's letter dated 21 February 2018.

114 The request and the confirmation are attached as appendix 3 to Uber's letter of 11 December 2017.

115 See the email attached as Appendix 3 to Uber's letter dated 11 December 2017.

116 This e-mail is attached to Uber's letter dated 21 February 2018.

program of Uber.117 In the opinion of the AP, Uber deliberately made this report differently than other vulnerability reports.

The HackerOne page of the Uber group states that the highest bug bounty is in a bandwidth
up to a maximum of $20,000. At the time of the data breach, a typical maximum of $10,000,118 was in effect
reporters have indicated that they want a “6 digits” bug bounty for sharing what they find
leak.119 While the $100,000 bug bounty paid through HackerOne in $10,000 instalments,
exceeds the limit of the indicated bandwidth, Uber declares that the amount to be paid
bug bounties is subject to the discretion of the Uber Group.
On February 6, 2018, at a subcommittee hearing, the [CONFIDENTIAL] of UTI
of the United States Senate. stated that the payment had the character of 'ransom' for it
remove the leaked data: “Our primary goal in paying the intruders was to protect our consumers’ data.”
He also states: “We recognize that the bug bounty program is not an appropriate vehicle for dealing with intruders
who seek to extort funds from the company. The approach that these intruders took was separate and distinct from those of
the researchers in the security community for whom bug bounty programs are designed. While using the bug bounty
program assisted in the effort to gain attribution and, ultimately, assurances that our users' data were secure, at the end of
the day, these intruders were fundamentally different from legitimate bug bounty recipients.”120
From the speed with which the $100,000 payment was agreed to, that a
substantially higher amount than usual, and the later statement of the [CONFIDENTIAL], appears
in the opinion of the AP that the management of UTI was aware of the seriousness of the data breach
at the time of that decision-making, and therefore felt compelled to provide the reporters with what they requested
amount to prevent further damage to Uber users.
3.5.3.3 Confidentiality
That UTI's management was aware of the seriousness of the data breach at the time of decision making
in connection with the handling of the reported data breach, in the opinion of the AP, it is also clear from the
additional agreements concluded with the reporters with the intention of keeping the data breach secret
at least with the intention of preventing public disclosure.
Confidentiality obligations and obligations to delete research data and no further
are not uncommon when reporting vulnerabilities to organizations and companies,

also known as 'responsible disclosure'. However, not all bug bounty programs require complete ones

secrecy of the investigation, some organizations make the findings of the researchers

public.

At the time of the data breach, it was Uber's policy in its HackerOne bug bounty program

that researchers were allowed to publish about the vulnerabilities they discovered after the vulnerability

117 Written response from Uber dated 12 January 2018 to AP questions, question 29.

118 Ditto.

119 This e-mail is attached to Uber's letter dated 22 December 2017.

120 See appendix to Uber's letter dated 7 February 2018.

Date

November 6, 2018

Our reference

[CONFIDENTIAL]

was solved by the Uber group. Fixed some of the bugs by the Uber group via HackerOne

vulnerabilities have been published by the Uber group itself. The Uber group has via a blog post

information about the first hundred days of its bug bounty program. In that blog post

also highlighted a number of vulnerabilities that have been resolved through the bug bounty program.121

In the present case, however, UTI has concluded additional agreements with the notifiers, which it

forbade the reporters to go public in any way whatsoever with what they discovered

data breach. This additional agreement supplemented the Uber group's policy for HackerOne, and

exhaustively arranged the agreement between the reporters and UTI where there were conflicts between the standard

policy of the Uber group and the agreement in question existed. A provision about

confidentiality is included in the agreement governing the payment of the bug bounty. In

this agreement stipulates that “[researchers] have not and will not disclose anything about the vulnerabilities or

your dialogue with us to anyone for any purpose without [UTIs.] written permission. This includes any analysis or post-

mortem in any medium or forum."

The agreement further states: "[Researchers] and [UTI[promise that if [researchers] break [researchers'] promises to [UTI]. [researchers] will repay to [UTI] the bounty reward.]"122

Further internal communication from UTI staff shows that the secrecy of the data breach by the reporters is deemed essential by UTI. In commentary on a paper on the handling of the data breach is written as follows: "ensuring that the research isn't written about, presented on, etc."123

Based on the above, the AP determines that UTI's management was aware of the severity of the data breach and it was important to her to keep the data breach a secret, at least to prevent publicity.

3.5.4 Seriously culpable negligence

As jointly responsible, both UTI and UBV were liable for the entirety of the data processing and related obligations. This rested on both UBV and UTI pursuant to Article 34a, paragraphs 1 and 2 of the Wbp, the obligation to report the data breach without delay to both the AP and those involved.

UBV and UTI, as jointly responsible, acted seriously culpably negligently by the not immediately report a data breach to the AP and those involved. That UBV and UTI have failed it to report a data breach to the AP in a timely manner and to inform those involved of the data breach in a timely manner is the result of grossly, significantly carelessly, negligently or injudiciously. The AP points out in this regard considered in relation to the following facts and/or circumstances.

First, as described above, UTI's management was already on November 14, 2016 level of the data breach. On that date, UTI's then [CONFIDENTIAL] received an e-

121 URL: https://eng.uber.com/bug-bounty-update/ (last accessed October 10, 2018).

122 The agreement is attached as appendix 3 to Uber's letter of 11 December 2017.

123 This quote follows from an e-mail appended to Uber's letter dated 10 January 2018.

Date

November 6, 2018

Our reference

[CONFIDENTIAL]

mail message from a person who informed the [CONFIDENTIAL] that he found a major vulnerability in the

data security of the Uber group.

Second, as described above, UTI's management acted almost immediately, at least shortly after

the initial report aware of the circumstances from which it reasonably follows that there is

a security breach leading to a significant risk of serious adverse consequences, or

has serious adverse consequences for the protection of personal data.

Thirdly, as described above, that of a large multinational company applies

like the Uber group, it may be expected that it adheres to the legal requirements applicable to it

obligations in the countries in which it operates. The AP assumes that UTI is aware of it

was that the obligation to report data breaches, as regulated in Article 34a Wbp, applied to it at the time of the

data breach. Least of all, UTI should have known about the obligation.

With reference to the violation part of this decision, the AP is of the opinion that UTI is already on 14

November 2016, at least no later than 72 hours after the discovery on November 14, 2016, the data breach to the AP

should have reported.

Despite the knowledge of the data breach, the seriousness of the data breach and the clarity of the applicable

legislation in mid-November 2016, the Uber group was apparently all about the data breach

to keep secret, at least to prevent public access and the data leak is only more than a year after

discovery of the data breach at UTI on November 21, 2017 reported by UBV to the AP. In light of it

the AP cannot conclude otherwise than that there is serious culpable negligence

on the part of UBV and UTI as jointly responsible.

Even if Uber were to be followed in its argument that only UBV should be responsible

are regarded and UTI as a processor, then according to the Policy Rules there is still a data breach notification obligation

It always applies that the data breach occurred on November 14, 2016, or at least no later than 72 hours after its discovery on November 14, 2016.

November 2016, should have been reported to the AP. In the Policy Rules reporting obligation data breaches is in this included that: “The period for reporting the data breach starts the moment you, or a processor you have engaged becomes aware of an incident that may fall under the data breach notification obligation.”

The opinion of UBV, that on 4 November 2017 a first meeting took place between UTI and UBV and that on 10 November 2017 UBV first became aware of the fact that it was downloaded files (also) concerned personal data of Dutch users, does not matter either the above judgment of the AP.

Under the processor agreement concluded between UTI and UBV on March 31, 2016, UTI was obliged “[to] promptly notify Uber B.V. about: (ii) any accidental or unauthorized access.”124 Considering the joint responsibility, the group relationship and Policy rules on the obligation to report data leaks, UBV can adhere to not excuse the AP's judgment with the fact that UTI failed to inform UBV.

124 Annex 1, Data Processing Agreement, to Uber's written response dated December 1, 2017.

Incidentally, the AP notes that the [CONFIDENTIAL] of UBV was informed on October 25, 2017 of what Uber calls in its view an “IT security incident in 2016, that it was being investigated, and that it could potentially create a media cycle.”125 In the opinion of the AP, UBV cannot have a justified appeal act on ignorance, which consists in the [CONFIDENTIAL] of UBV not having “knowledge of the scope of the incident, or if personal data was involved” had126. With the information that was known on October 25, 2017 at the [CONFIDENTIAL] of UBV – an IT security incident that could potentially attract media attention cause - in the opinion of the AP it was reasonably on its path to continue critically

questions in order to find out whether there was a data breach, or whether personal data were involved involved and what the relevance of the IT security incident was for UBV. By failing to do so, UBV equally seriously culpably negligent.

Even if the AP were to agree with UBV's view, namely that on November 10, 2017 it first took note of the downloaded files with personal data of Dutch users and should therefore have reported it to the AP no later than 72 hours after that knowledge, the The AP has established that UBV reported the data breach far too late with its report on November 21, 2017.

The AP also finds that UTI and UBV wrongfully failed to notify those involved without delay prescribed manner of the data breach.

The AP sees no reason for the other circumstances put forward by Uber in the opinion another judgement. No later than 72 hours after the discovery of the data breach on November 14, 2016, the data breach should have been reported to the AP and those involved should have been informed of the data breach be made.

3.5.5 Conclusion

In the opinion of the AP, all of the above shows that UTI and UBV grossly, significantly negligently, have acted negligently or injudiciously, as a result of which there is serious culpability negligence on the part of UBV and UTI.

4.

4.1

As noted in the previous paragraph, the AP will determine the amount of the fine for the apply the most favorable provision to the offender by joining the fine regime of the Wbp. In the below, the AP will first briefly explain the penalty system, followed by the determination of the fine in this case.

4.2

According to Article 66, second paragraph, of the Wbp, in the event of a violation of Article 34a, first and second paragraph, of the Wbp a fine not exceeding the amount of the sixth category of article 23, fourth paragraph,

of the Criminal Code. According to article 23, fourth paragraph, of the Penal Code, it amounts to maximum of the fine of the sixth category as of 1 January 2016: € 820,000.

125 Annex 1 to Uber's written opinion dated 3 July 2018.

126 Ditto.

Amount of the fine

The system

Introduction

37/42

Date

November 6, 2018

Our reference

[CONFIDENTIAL]

The AP has established 'Fining Policy Rules for the Authority for Personal Data 2016' (Fining Policy Rules) regarding the interpretation of the power to impose an administrative fine, including determining of the level thereof.127 In the Fining Policy Rules, a categorization and bandwidth has been chosen system.

The fineable provisions, the compliance of which is supervised by the AP, are per statutory maximum fine of € 820,000, € 450,000 or € 20,500 divided into a number of fine categories, and linked to them in increasing fine bandwidths.

The fine categories are arranged according to the seriousness of the violation of the aforementioned articles, where category I contains the least serious offenses and category II or III the most serious offences.

Violation of Article 34a, first paragraph, Wbp and violation of Article 34a, second paragraph, Wbp are both classified in category II.

Within the bandwidth, the AP sets a basic fine. The starting point is that the AP sets the basic fine set at 33% of the bandwidth of the fine category linked to the violation.128

The AP then adjusts the amount of the fine to the factors referred to in Article 6 of the

Penalty policies, by lowering or increasing the base amount. In principle, within the

bandwidth of the fine category linked to that violation. It's an assessment

of the seriousness of the offense in the specific case, the extent to which the offense is imposed on the offender

can be blamed and, if there is reason to do so, other circumstances, such as the (financial)

circumstances in which the offender finds himself. The AP can do so, if necessary and depending on the degree

in which the factors referred to in Article 6 of the Fining Policy Rules give rise to this, the

Apply penalty bandwidth of the next higher or the next lower category respectively.

4.3

It follows from Appendix 1 to Article 2 of the Fining Policy Rules that the violation of Article 34a,

first paragraph of the Wbp and the violation of article 34a, second paragraph, Wbp are classified in category II. The

AP sets the basic fine for violations subject to a statutory maximum fine of € 820,000 and

which is classified in category II fixed within a fine range between € 120,000 and € 500,000. In this

case, the basic fine per violation is set at € 246,500.

Severity of the violation

According to Article 6, paragraph 1, of the Policy Rules, the AP takes into account the seriousness of the violation. Bee

the DPA considers, among other things, the nature and extent of the violation when assessing the seriousness of the violation

The categorization and the basic fine

127 Policy rules of the Dutch Data Protection Authority of December 15, 2015, as last amended on July 6, 2016, with regard to

imposing administrative fines (Fine Policy Rules of the Dutch Data Protection Authority 2016), Stcrt. 2016, 2043.

128 Fining policies, p. 10-11.

violation, the duration of the violation and the impact of the violation on those involved and/or the

society.129

Pursuant to Article 34a, first paragraph, Wbp, as that provision applied at the time of the violation, the
responsible to immediately inform the AP of a security breach, referred to in
Article 13 Wbp, which leads to the considerable chance of serious adverse consequences or serious adverse consequences
has consequences for the protection of personal data.

Pursuant to Article 34a, second paragraph, Wbp, as that provision applied at the time of the violation, the
responsible to immediately inform the data subjects of a security breach, if
the breach is likely to have adverse consequences for his privacy.

The purpose of the reporting obligation is to prevent data leaks and, if they do occur, the consequences
as much as possible for those involved. The duty to report contributes to the
maintaining and restoring trust in the handling of personal data.130

Transparency about the nature of the data breach, its probable size and nature of the possible
damage, the efforts made to repair the damage and advice to the public and
customers to enable themselves as best as possible to bear the consequences for their own interests
oversee the necessary measures to maintain and restore that confidence. That confidence
is supported by the fact that the AP must be enabled to form its own picture of the
facts, to be able to give an opinion on the measures taken, under certain circumstances confidentially with
to be able to consult the person responsible and to intervene if necessary.131

For the sake of completeness, it is noted in this respect that, having regard to recitals 85 to 88 of
the preamble to the GDPR, with the notification obligation based on Articles 33 and 34 GDPR having a similar purpose
is pursued.

In the period from November 15, 2016 to at least November 21, 2017, UBV and UTI failed to
to immediately inform those involved of the data breach. It was not until November 21, 2017 that UTI released the
informed by means of a news report. As a result, those involved are unable to do so (in time).
to oversee the consequences for one's own interests, for example by being alert to the risk of
(spear)fishing. In addition, those involved do not have, or at least did not have timely,

can take precautions to mitigate potentially adverse consequences of the data breach. This considers the AP serious.

When assessing the seriousness of not immediately reporting the data breach, the AP also has the size of the data breach taken into account. The data breach affects a large number of people, 57 million stakeholders worldwide and 174,000 Dutch stakeholders. Only the size of the data breach had UTI and UBV must give cause to inform the AP and those involved. The data breach also concerns a large amount of personal data including names, email addresses and mobile phone numbers. These circumstances mean that the data breach has serious adverse consequences for the

129 This is incidentally in line with the criterion from Article 83(2)(a) GDPR.

130 Parliamentary Papers II 2012/13, 33 662, no. 3, p. 1.

131 Parliamentary Papers II 2012/13, 33 662, no. 3, p. 4.

protection of personal data, or at least could have. In the opinion of the AP, it is through the violation has seriously damaged confidence in the handling of personal data.

In addition, UBV and UTI will, in any case, have until 72 hours after discovery of the data breach on November 14, 2016. November 21, 2017, failed to notify the AP of the security breach. Thus it is the AP was not aware of the (extensive) data breach for a longer period of time. The AP has therefore not (in time) been able to form its own picture of the facts and the possible actions by Uber measures taken, both towards those involved and with regard to the necessary handling of the (acute) security breach. This failure of UTI and UBV has severely hampered the AP in her supervision, which indirectly also affects the interests of those involved.

On balance, the AP sees reason to adjust the basic amount of the fine, based on the degree of seriousness of the offense

violation, to be increased by one third per violation to €327,845.

Degree of culpability of the offender

According to Article 6, paragraph 2, of the Policy Rules, the AP takes into account the extent to which the violation can be attributed to the offender.132 If the violation was committed intentionally or the is the result of seriously culpable negligence as referred to in Article 66(4) of the Wbp assumed that there is a considerable degree of culpability on the part of the offender.

As the AP has already explained above, the AP is of the opinion that there is serious culpability negligence on the part of UTI and UBV. In short, it comes down to being within the top of the Uber group was aware of the data breach, they were aware of its seriousness and there there could be no misunderstanding that the AP and those involved were immediately aware of the data leak must be stated. Nevertheless, the Uber group was committed to keeping the data leak a secret hold, for which Uber has been prepared to pay a substantially higher amount of money than usual pay to reporters and to agree additional confidentiality obligations with the reporters.

Only more than a year after the discovery of the data breach at UTI, the data breach was discovered by UBV on November 21, 2017.

reported to the AP and a news item was published on Uber's website by the current CEO of UTI informing the public about the data breach. In view of the foregoing, the AP is of the opinion that there is a considerable degree of culpability.

The AP therefore sees reason to set the basic amount of the fine, based on the degree of culpability per violation by one third.

With the previous steps, the fine amount comes to € 409,190 per violation, so that the total fine would amount to € 818,380.

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

132 This is incidentally in line with the criterion from Article 83(2)(b) GDPR.

of the fine, given the circumstances of the specific case, does not lead to a disproportionate outcome.

Application of the proportionality principle is possible according to the Fining Policy Rules of the AP, among other things play in the accumulation of sanctions. If the AP for distinguishable, but related wants to impose two or more fines for violations, the total of the fines must still match the seriousness of the violations.133

In this case, the AP proceeds to impose a fine for violation of both Article 34a, first paragraph and second paragraph member of the Wbp. In the opinion of the AP, these are separate violations. After all, article 34a, paragraph 1 of the Wbp requires that the AP be notified immediately of a data breach while Article 34a, second paragraph, of the Wbp requires that the data subjects are immediately notified of a data breach. At the same time, the AP recognizes that the essence of the relevant provisions is equivalent, namely transparency with a view to building trust in dealing with retain and/or restore personal data. Furthermore, the AP is of the opinion that the conduct that the underlying offenses are essentially based on the same set of facts. This gives reason to moderate the above-mentioned fine amount on the basis of proportionality.

In assessing proportionality, the AP also takes into account the fact that, despite the the passage of time and the absence of a binding indication, the data breach is ultimately public and its settlement has received the necessary media attention so that those involved are aware of it have been able to take.

The AP thus sets the total fine amount at € 600,000. This amount can Uber given its financial carry position.

5.

The AP will jointly submit to the UBV and UTI, due to violation of Article 34a, first and second paragraph, Wbp, an administrative fine in the amount of € 600,000, for the payment of which they are jointly and severally liable are.

UBV and/or UTI must transfer the amount to a bank account within six weeks [CONFIDENTIAL] on behalf of the Dutch Data Protection Authority, stating the case number [CONFIDENTIAL]. UBV and UTI will not receive a separate invoice for this amount.

The fine must be paid within six weeks of the date of this decision.134 If UBV and/or UTI object(s) to this decision, the obligation to pay the fine is suspended until the objection has been resolved. That obligation is also suspended if UBV and/or UTI after the objection procedure appeals, until a decision has been made on the appeal.135

Operative part

133 Fining policies, p. 11.

134 See Article 4:87(1) and Articles 3:40 and 3:41 of the Awb.

135 See article 71 Wbp.

Date

November 6, 2018

Our reference

[CONFIDENTIAL]

The Dutch Data Protection Authority,

On their behalf,

e.g.

Mr. A. Wolfsen

Chair

Remedies Clause

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

decision to submit a notice of objection to the Dutch Data Protection Authority, PO Box 93374, 2509 AJ The Hague, stating “Awb objection” on the envelope.