Registered mail

[CONFIDENTIAL]

Date

Nov 6, 2018

Our reference

[CONFIDENTIAL]

Contact

[CONFIDENTIAL]

Topic

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

authority data.nl

Dear Sirs [CONFIDENTIAL],

The Dutch Data Protection Authority (AP) has decided to inform your clients about Uber B.V. (UBV) and Uber Technologies, Inc. (UTI) jointly impose an administrative fine of €600,000, because UBV and UTI, as (joint) 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 to notify data subjects of the data breach.

The notification to the AP first took place on November 21, 2017. On the same day, Uber issued a news item about the data breach on its website. This means that the AP and those involved are not immediately informed 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. Section 1 sets out the facts underlying

depend on the decision. Section 2 describes the legal framework. In section 3, the AP assesses its jurisdiction, responsibility for data processing, violations and serious culpable negligence. Section 4 elaborates on the amount of the administrative fine. Paragraph 5 contains the operative part and the remedies clause.

1

Date

Nov 6, 2018

Our reference

[CONFIDENTIAL]

Legal entities involved

Facts and process

1.

1.1

Uber B.V.

UBV is one of the Mr. Treublaan 7, (1097 DP) in Amsterdam with registered private limited company. 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 has its registered office at 1455 Market Street, San Francisco, United States. UTI is the ultimate parent company of a group of dozens of companies, including UBV.

UTI and UBV are hereinafter jointly referred to as “Uber” or as “Uber Group”.

1.2

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

Process sequence

As a result of that notification, the AP is an ex officio investigation started. In that context, a first written request for information was submitted on 23 November 2017

sent to UBV. Several further information requests followed. Uber has followed suit

given.

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

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

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

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

administrative fine and the report drawn up for it.

On July 11, 2018, a hearing was held 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 representative sent a further document to the AP.

1 Attribute [CONFIDENTIAL]

2 Investigation report [CONFIDENTIAL]

Date

Nov 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 allows 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

order (riders) are linked to drivers (drivers) who use another application of the Uber

concern customers (the Uber Driver app). Uber drivers use their own car for it

offering taxi rides are not employed by Uber and may increase the demand for taxi rides from Uber riders

accept or refuse.

To use the Uber apps, either 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 the processing of this data is, among other things, to bring questions and

offer to/from taxi rides and the processing of payments for those taxi rides.

1.4

UBV and UTI concluded a 'Data Processing Agreement' on March 31, 2016.

In it, UBV and UTI have agreed that UBV is responsible for the processing of

personal data 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 the United States will be

forwarded from the Netherlands to the United States. There they are stored on UTI . servers

in the United States. It has also become apparent that UTI has concluded a processor agreement for the use of data

storage capacity/servers (AWS S3) is contracted with Amazon. The purpose of that storage is to create

back-ups of that (personal) data.

1.6

On November 14, 2016, UTI was notified of a vulnerability in its data security. on

that date, the then [CONFIDENTIAL] of UTI received an email from a person who had the

[CONFIDENTIAL] informed that he and his team (reporter/reporters) identified a major vulnerability in the

data security of the Uber group.

The reporter had access to AWS S3 storage in the period from October 13, 2016 to November 15, 2016

from the Uber group using credentials stored in a private GitHub

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

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

1 UserID;

2 DriverID;

3 First and Last name;

4 E-mail address;

5 Mobile number;

Data breach and notification to AP

Date

Nov 6, 2018

Our reference

[CONFIDENTIAL]

6 Last confirmed mobile number;

7 Nickname;

8 Driver's license number;

9 Receipt email;

10 Tokens;

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;

22 Notes;

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 score.

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

The data breach prompted UTI to call in [CONFIDENTIAL], a forensic expert. It request for this was made on October 18, 2017. [CONFIDENTIAL] 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 It has been established that the data breach involved 57,383,315 Uber users, of whom 25,606,182 were US - and 31,777,133 non-US. Information from UBV shows that approximately 174,000 Dutch Uber users have been affected by the data breach. The investigation conducted by [CONFIDENTIAL] shows that 31 types of personal data were involved in the data breach.

On October 25, 2017, the [CONFIDENTIAL] of UBV 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 of January 10, 2018, [CONFIDENTIAL].

Date

Nov 6, 2018

Our reference

[CONFIDENTIAL]

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

UTI announced that there was a security incident.

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

UTI informing the public about the data breach.4 On the same day, UBV notified

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 notification by

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

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

95/46/EG5, was repealed on May 25, 2018.6 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 it is relevant, and

explained. Subsequently, in subsection 2.2 the legal framework under the GDPR, insofar as relevant,

described.

2.1

2.1.1

Article 1, preamble and under a, of the Wbp provides that personal data is any data relating to a

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

understood. To determine whether a natural person is identifiable “all means must be taken”

which may be assumed to be reasonably provided by the controller or

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

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

or any set of actions relating to personal data, including in any case the

collect, record, organize, store, update, modify, retrieve, consult, use,

provide 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

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

6 In Article 51 of the General Data Protection Regulation Implementing Act (UAVG) – which entered into force with effect from

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

7 Article 99(2) of the GDPR provides that the GDPR applies from 25 May 2018.

8 By Royal Decree of 16 May 2018 (Staatsblad 2018, 145) the date for establishing 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 is

time to be determined by royal decree has been made possible.

9 Recital 26 Directive 95/46/EC (Data Protection Directive).

Date

Nov 6, 2018

Our reference

[CONFIDENTIAL]

Scope of application Wbp

bringing together, associating, as well as shielding, erasing or destroying

data.

2.1.2 Responsible

Article 1, preamble and under d, of the Wbp provides that the responsible person is the natural person, legal person or any other person or administrative body which, alone or jointly with others, has the object of and the means of processing 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 affect the individual responsibility of one of the (joint) responsible persons.10

2.1.3

Article 4(1) of the Wbp provides 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 provides 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 that are located in the Netherlands unless these means are only used for the transfer of personal data.

2.1.4

Article 13 of the Wbp stipulates that the responsible party must provide 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 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, first paragraph, of the Wbp stipulates that the person responsible must inform the Board (read: informs the AP) without delay 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./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 Conclusion that 'joint responsibility' in the sense of the Directive can be interpreted broadly, in the sense that various variants and division of tasks are possible and also that when determining

the division of responsibilities in a legal sense the way in which entities actually work together in practice a decisive criterion. See: Opinion AG Bot, case C□210/16 (Wirtschaftsakademie Schleswig-Holstein), 24 October 2017, par. 46-51 and subsequent CJEU judgment, C□210/16, 5 June 2018, ECLI:EU:C:2018:388.

11 In its Guidelines on the security of personal data, the AP (at that time the Personal Data Protection Authority) has elaborated on what should be understood by 'appropriate technical and organizational security measures'. In addition, connected to standards, methods and measures that are customary in the field of information security. See CBP Guidelines for the Security of Personal Data, February 2013, URL: https://autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-publiceert-guidelines-security-of-personal-data.

12 Royal Decree of 1 July 2015 (Stb. 2015, 281).

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 provides that the controller shall immediately inform the data subject of the infringement referred to in Article 34a(1) of the Wbp, if the infringement is probable will have an adverse effect on his privacy.

In its Policy Rules on the obligation to report data breaches, the AP has further elaborated on how responsible parties

should give substance to the obligation to report data breaches, and provides tools to those responsible for determine whether they have to report certain security incidents to the AP under the data breach reporting obligation report.13 The Policy Rules on the obligation to report data breaches also contain an interpretation of the obligation to notify involved. 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 provides, insofar as relevant, that the AP may impose an administrative fine the imposition of a maximum of the amount of the fine of the sixth category of Article 23, fourth paragraph, of the Criminal Code with regard to violations of the provisions of Article 34a of the Wbp. Article

23, seventh paragraph, of the Criminal Code applies mutatis mutandis.

Article 66(3) of the Wbp provides, insofar as relevant, that the AP does not impose an administrative fine because of 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 given a binding instruction. The AP can give the offender a term within which the instruction must be followed.

Article 66(4) of the Wbp provides 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(1) of the GDPR provides that if a personal data breach has occurred occurred, the controller reports it without undue delay and, if possible, no later than 72 hours after becoming aware of it, to the competent supervisory authority, unless it is not probable that the infringement 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 leaks in the Personal Data Protection Act (Wbp)' of 8 December 2015 (Government Gazette 2015, no. 46128).

Article 33(2) of the GDPR provides that the processor must notify the controller without unreasonable delay as soon as it becomes aware of an infringement related to personal data.

2.2.2 Communication of a personal data breach to the data subject

Article 34(1) of the GDPR provides that where the personal data breach likely to pose a high risk to the rights and freedoms of natural persons, the controller the data subject the personal data breach without undue delay shares.

2.2.3

Article 83(1) of the GDPR provides that each supervisory authority shall ensure that the administrative fines imposed under this article for the activities referred to in paragraphs 4, 5 and 6 infringements of this Regulation are effective, proportionate and dissuasive in each case.

Administrative fine

Rating

Article 83(4) of the GDPR provides 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, whichever is higher.

3.

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

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

violation of Article 34a(1) of the Wbp is established in subsection 3.3. The violation

of Article 34a, second paragraph, of the Wbp is established 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 is

Notified 14 Nov 2016. 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 addressed a first written request for information to the UBV. The final de

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

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

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 Authority for Personal Data

Period of conduct

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

Date

Nov 6, 2018

Our reference

[CONFIDENTIAL]

3.1.2 GDPR as the basis for the fine

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

UBV on 21 November 2017, the Wbp applied. The Wbp, which was the implementation of Directive 95/46/EG15, is withdrawn on 25 May 2018.16 The GDPR also came into effect on that day17 and the UAVG in came into effect.18

The GDPR replaces Directive 95/46/EG19 and the Wbp. Where the GDPR provides scope for further rules state, these are laid down in the UAVG. According to the considerations to the GDPR, the objectives and principles of Directive 95/46/EC have been maintained.20 Both Directive 95/46/EC and the Wbp and the GDPR seek to protect the fundamental rights and freedoms of natural persons in relating 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 - remained the same as those from Directive 95/46/EC and the Wbp.

In this case it is important that under the regime of the Wbp as well as that of the AVG 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 reporting obligation laid down in 34a, first and second paragraph, of the Wbp and in the GDPR in Article 33, first paragraph and Article 34, first paragraph. These provisions aim to safeguard the same legal interests. The authority to the imposition of an administrative fine due to a data breach is regulated in the Wbp in Article 66, second paragraph, of the Wbp and in the GDPR in Article 58, second paragraph, preamble and under i, read in conjunction with Article 83, fourth paragraph of the GDPR. There is no question of a (substantial) material change in the regulations. Also there is no different opinion about the criminality of the duty to report as such.22 This is the case of an uninterrupted legal order. This means that, in order to guarantee the continuity of the legal order, for conduct that - as in the present case - took place under the regime of 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 Nov. 1995, No. L 281/31 (the so-called Privacy Directive).

16 Article 51 of the UAVG – which entered into force on 25 May 2018 – states that the Wbp will be repealed.

17 Article 99(2) of the GDPR provides that the GDPR applies from 25 May 2018.

18 By Royal Decree of 16 May 2018 (Staatsblad 2018, 145) the date for establishing 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 is 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 regulation on a duty to report data breaches, it is apparent from 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, inter alia, Directive 95/46/EC, a regulation for regarded the obligation to report data breaches as an imperative requirement in the public interest. Legislative history also shows that with
the introduction of the notification obligation was intended to prevent processing of personal data in violation of Directive 95/46/EC
(Parliamentary Papers II 2012/13, 33 662, no. 3 Reprint, p. 14.)

22 However, the threat of punishment has changed.

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

Date

Nov 6, 2018

Our reference

[CONFIDENTIAL]

In a case where the continuity of the legal order is at issue, it is, in so far as relevant here,
tested against substantive law as it applied at the time when the conduct24 took place.25 In this
this is the case with the Wbp, more specifically Article 34a, first and second paragraph. This also means that
affiliated with the 'more favorable' fine regime for the offender compared to the GDPR under the Wbp.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 regime of the Wbp this is, in view of
Article 66, paragraphs 2, 3 and 4, of the Wbp, was in principle a maximum of € 820,000.28
Under the GDPR, the notification obligation can be fined on the basis of Article 58, second paragraph, preamble and
under i, viewed in conjunction with Article 83, fourth paragraph, under a. As the AP explains in more detail in this decree,
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
GDPR have resulted in a violation of Articles 33(1) and 34(1) of the GDPR.

3.1.3 Wbp as a basis of jurisdiction; transitional law UAVG

Transitional law is provided for in Article 48, eighth paragraph, of the UAVG. Under that provision,
legal procedures and legal proceedings that the Dutch Data Protection Authority29 has previously initiated
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 derives the AP the power to impose an administrative fine also from the Wbp. It
this concerns a legal procedure in which the DPA 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 AVG and the entry into force of the UAVG. Also the AP
prepared report of 1 June 2018 and (the procedure that led to) this decision are part

24 It is noted that conduct also includes an omission, such as in the present case not immediately reporting a
data breach.

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

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

26 In Section 5:46(4) of the Awb, Section 1, subsection 2 of the Criminal Code will apply mutatis mutandis declared. Pursuant to Article 1, second paragraph, of the Criminal Code, in the event of a change in legislation after the time on 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 on changes in legislation with regard to the threat of punishment applies that 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 GDPR.

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 fine for a data breach after a binding instruction was given, unless the violation was intentional committed or was the result of grossly culpable negligence.

29 Formally, the name change from the Dutch Data Protection Authority to the Dutch Data Protection Authority was first formally announced at the UAVG implemented although the name of the Dutch Data Protection Authority has been used in society for some time.

Conclusion on jurisdiction of this legal procedure. This means that on the basis of 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
do not immediately report a data breach to the DPA - is authorized on the basis of Article 48, eighth paragraph, 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 power from Article 58, second paragraph, preamble
and under i, in conjunction with Article 83(4)(a) of the GDPR30 for violation of the
reporting obligation referred to in Article 34a(1) of the Wbp and as included in . since 25 May 2018
Article 33, first paragraph and Article 34, first paragraph 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 purpose 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 responsible. The
after all, the responsible party is the standard addressee.
'Controller' within the meaning of Article 1, preamble and under d, of the Wbp, is understood to mean:
Data controller
Introduction
‘the natural person, legal person or any other 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 - which
constitutes the implementation of the concept of “controller” from Article 2(d) of
Directive 95/46/EC - consists in ensuring effective and complete protection of data subjects
insure through a broad description of the term 'responsible person'.32
In this regard, it should be noted that the GDPR in Article 4, seventh paragraph,
'controller' defines (materially) equivalently as Directive 95/46/EC and the Wbp.

3.2.2 UBV formal-legal responsible

In answering the question of who is responsible, the formal legal authority to:

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

corporate relationships, as discussed here, the legal person under whose jurisdiction the

30 This power is enshrined in national law in Article 14(3) of the UAVG.

31 This description, insofar as relevant, corresponds 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

habitats

persons in connection with 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, paragraph 34 (ECLI:EU:C:2014:317) and CJEU 5 June 2018,

Wirtschaftsakademie Schleswig-

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

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

operational data processing takes place as the responsible party.34 In the

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

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 designated therein as a processor ('processor')36 that is used for the benefit of UBV

processes personal data.37 The DPA is of the opinion that it can be inferred from this that UBV has the formal

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

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

As is further substantiated below, this does not exclude the possibility that, in addition to UBV, also UTI as responsible can be designated.

3.2.3 UBV and UTI are jointly responsible

The AP is of the opinion that UBV not only, but together with UTI, aims and means for the processing of personal data. UBV and UTI are therefore jointly responsible to notice. Each of those responsible, both UTI and UBV, is liable for the entirety of the data processing and compliance with the associated obligations.38 In the following, motivates the AP takes that position and also includes Uber's view on the report of the AP. Uber itself considers UBV as the - sole - responsible party.39

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

Although UBV has formal legal control on the basis of the processor agreement, this is not by definition decisive for the question whether UBV is (solely) responsible. As the Article 29-working group - the independent advisory and consultation body of European privacy regulators and currently referred to as the European Data Protection Board - noted in its opinion of 16 February 201040, the provisions in a contract often provide greater clarity, but they are not always decisive. The term “controller” is a functional term, intended to define responsibilities place where the actual influence lies.41 Based on this factual assessment, the AP that UTI and UBV (jointly) make decisions regarding the establishment of goals and data processing resources.

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 processor agreement (especially considerations A to D).

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

had eyes.

39 Written response from Uber dated 1 December 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 as conclusion 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.

With regard to UTI it concerns:

- The joint determination of the purpose of the data processing;
- Adoption of the information security policy;
- decisions about data storage, and
- Developing and providing the Uber app as well as performing updates.

These factors will be explained below.

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

UBV and UTI primarily determine the purpose of the processing of the personal data. In the letter of 7 February 2018, Uber declares that the drafting of the privacy statement is a joint effort of UBV and UTI.42 It appears from the introductory paragraph of the privacy statement 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 the purposes for which the information may be processed. 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.

The personal data processed by the Uber group is backed up that

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 concerned personal data in the backups stored in the

(external) AWS S3 storage.44

From the foregoing, the AP concludes that UTI and UBV 'jointly' fulfill the purpose of the processing of

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 event if it becomes responsible for the processing

45 Now it appears from the foregoing that UTI and UBV jointly fulfill the purpose of the processing of

personal data, they are already jointly responsible on that ground.

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 15 July 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

Nov 6, 2018

In addition to the purpose, UTI also (partly) determines the means for the processing. In this regard, it is important to notice that even if someone merely determines the means, he can be responsible. The Article 29-working group indicates in its above-mentioned advice that when determining the resources only of responsibility arises when that determination relates to the essential aspects of the resources.46

The Uber group, of which UBV and UTI are part, has a global 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 are included, has been determined by UTI.47 This includes, for example to take measures regarding 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 information security, 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 in themselves be delegated to a processor.50

The AP is of the opinion that UTI thereby establishes an essential aspect of the resources and this (partly) contributes to this contributes that UTI, together with UBV, determines the purpose of and the means for the processing of personal data 51 Nevertheless, the AP emphasizes that - as explained above - UTI (partly) serves the purpose of the processing and can therefore already be jointly responsible with UBV qualified.

Uber view and AP response

With regard to its working method, Uber notes in its view that the controller determines how and why

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

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

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

Technologies, Inc.”. In the Information Security Policy Version 0.1 of August 31, 2016, the front page reads as the author “Uber Inc.”

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

The subsequent March 2017 Information Security Policy will have UTI on the front page. 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, for example, decides for whom the processed data

must be accessible if responsible can be designated (recommendation 1/2010 on p. 18).

49 Information Security Policy version 0.1, August 31, 2016, p. 5 (See also AP report of 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 advice 1/2010 on p. 17 Note that in some legal systems, security measures expressly

be considered an essential feature.

Date

Nov 6, 2018

Our reference

[CONFIDENTIAL]

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

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". The AP notes that in the letter from the
Dutch DPA from 2002 explains 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 opinion of the AP, it is not possible to conclude from the contents of this letter
that the way in which UTI in particular (actually) operates should lead to the conclusion that UBV and UTI
cannot be regarded as jointly responsible. On the contrary, as before
noted, UTI also determines the purpose and means of the processing.
In its view, Uber further cites a passage from the guidelines of the ICO, from which, according to Uber
it appears that a processor has a certain discretion about details of the execution of
processing of data. An example is given in the guidelines of a bank that is an IT company
enables data storage.
In response, the AP notes that this example does not justify the conclusion that UTI is not
can be regarded as jointly responsible. The role of UTI is as explained below:
beyond the mere provision of storage as referred to in the guidelines of the ICO
example. Moreover, being jointly responsible is also determined by handling
of a uniform privacy policy and the establishment of the information security policy by UTI as well as
the development, offerings and updates of the Uber apps to be discussed below and the handling of the
data breach by UTI.
Storage of the 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 herein that use is made of the Amazon storage service AWS S3. In that
connection has also been chosen by UTI for the United States as the location for that storage, whereby

[CONFIDENTIAL].

52 Written response UBV dated 12 January 2018, p. 6, answer to question 8.

Date

Nov 6, 2018

Our reference

[CONFIDENTIAL]

The AP concludes from the above that UTI is committed to the storage of personal data autonomously 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 (actually) a large 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 combined with the other facts and circumstances - applying a uniform privacy policy, determining the information security policy as well as the development, offering and updates of the Uber apps, and the handling of the data breach by UTI - that UTI and UBV are jointly responsible to be.

Uber view and AP response

In its view on the surcharge, Uber states that it does not agree with the conclusion of the AP that UTI de determining influence of UTI on the location and implementation of the data storage as an indicator can be seen to designate UTI as responsible for data processing. She points out that the processor agreement allows storage by UTI and that UTI as a 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 well as between UBV and UTI. According to UTI, this is also a common construction.

In this regard, the AP notes that the fact that the storage of personal data by UTI is possible on the basis of the processor 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 that

would be irrelevant to the question of whether UBV and UTI can become jointly responsible

designated. 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 storage without including UBV

know. Nevertheless, 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, offering and updates

The Uber group offers a service that allows users to

developed app (Uber app) to purchase passenger transport. Users are linked to a

driver (driver) who can take on customers via another app (Uber Driver app). The special

developed mobile applications are essentially the core service of the Uber group.53 UTI54 has the

Uber app - which serves as the basis for other apps - has developed and has licensed UBV to use the app

while also updating the Uber app by UTI. 55 UTI . thus contributes

contribute to the determination of the purposes 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") of 15 July 2015.

54 And her forerunners.

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

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

point of view - is responsible for adding new functionalities, does not do that

off. Rather, it emphasizes joint responsibility. The fact that UTI developer,

being a provider and executor of updates to the Uber app is still one of the elements that is relevant

for the question of 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 are not relevant, or do not determine who is the processor or

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 connection with this, the AP notes that the actual decisions about the handling of the data breach - about which UBV

was informed almost a year after the data breach took place - independently and solely by the

personnel from UTI have been taken. There are by the [CONFIDENTIAL] of UTI, without mentioning UBV herein

know and give her the opportunity to influence it, specific and important

measures taken. These measures concern the encryption of files in the AWS S3 buckets and

requiring two-factor authentication for services that the Uber group uses and that

be accessible via the internet.57

Uber's statement in its view that UTI's independent handling of the data breach without

Involving UBV in this only demonstrates that UTI is not fulfilling its obligations under the agreement

fulfilled, the AP does not follow. Uber thereby misunderstands that this factual course of action is precisely the conclusion of

the AP confirms that UTI makes decisions independently and thus has de facto control over the way

on which a data breach is handled.

UTI also has - as Uber states in issue 2.23 of its opinion - law firm

[CONFIDENTIAL] Requested to engage [CONFIDENTIAL], an outside forensic expert. Also

in this case, UBV is not known in advance (or immediately afterwards). That according to Uber - as it sees it states - it was logical that UTI conducted an independent investigation because the incident related to more US users than Dutch or any other country users and UTI de 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 necessary for storage of personal data in the United States also includes personal data collected and processed from data subjects outside the United States and according to the processor agreement UBV responsible.58

57 See more specifically section 4.3.4 of the report and the sources mentioned in footnotes 101 and 102 from there Uber.

58 Written response Uber dated February 7, 2018, p. 2, answer to question 1.

Date

Nov 6, 2018

Our reference

[CONFIDENTIAL]

UTI has issued a statement to the notifiers of the data breach for the protection of user data59 reward paid. This concerns a considerably larger amount than is usually paid.60 UBV is not involved and not known in the decision-making process. The closed in this connection with the reporters agreement is signed by UTI personnel and on behalf of UTI. UBV was out there.

Uber view and AP response

In its opinion, Uber notes that the payment to the reporters and the agreement concluded with them is not an 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. It has been made known by the [CONFIDENTIAL] of UTI 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 being allowed to be an editor expected.

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

The AP notes in this regard that the way in which UTI actually operates and makes decisions where it is the handling of the data breach is one of the factors that is relevant to the question of whether UTI is jointly responsible. The role that UTI plays in handling the incident therefore does not stand alone.

3.2.4 Conclusion jointly responsible

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 heed of the processor agreement, whereby UBV is designated as the controller. Furthermore, it has been found that UTI has determined the purpose of the data processing together with UBV, UTI itself has established information security policy, has made important decisions independently regarding the storage of personal data and has developed and offers the Uber app and updates for it. The judgment of the AP is further strengthened by the independent way on which UTI settled the data breach in question. The joint responsibility brings with understand that each of those responsible, i.e. both UTI and UBV, is liable for the entirety of the data processing and compliance with related obligations. In this regard, notes the AP notes that UTI and UBV can also be jointly responsible under the AVG regime designated.

3.3

59 Written response from Uber dated 7 February 2018, appendix “Testimony Uber (201826).pdf”, p. 5.

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

Introduction

3.3.1

As appears from subsection 2.1.5, as of 1 January 2016, pursuant to Article 34a(1) of the Wbp an obligation to report data leaks to the AP. Pursuant to this reporting obligation, the responsible party must inform the AP to notify without delay of a security breach, as referred to in Article 13 of the Wbp, which leads to a significant risk of serious adverse effects or has serious adverse effects on the protection of personal data. This obligation to report contributes to the preservation and restoration trust of the public, customers, the market, government and regulators in the relevant institution or company when handling personal data.61

3.3.2 Controller is standard addressee

It has been explained with reasons that UBV and UTI are jointly responsible brands. Both are jointly responsible for compliance with the Wbp for the whole of the processing. Both UBV and UTI are therefore obliged to report a data breach without delay to which Article 34a(1) of the Wbp pertained. Uber's statement in its view that the reporting obligation does not apply to UTI because UTI is not responsible - and therefore no standard addressee - the AP therefore deems it incorrect.

3.3.3

Article 34a, first paragraph, of the Wbp referred to a security breach as referred to in Article 13 Wbp (now Article 32 of the GDPR). Article 13 concerned a security regulation to which the

responsible had to abide and was directed 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 this case

as set out below, unauthorized persons outside the Uber group have access to the

data storage from Uber. This allowed them to download files with which they had access to,

and be able to take cognizance of personal data. Thus there was a form of unlawful

processing.

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

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

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

there was a breach of security within the meaning of Article 34a Wbp'.63 In this regard, it should be noted that

UTI forensic expert [CONFIDENTIAL] has commissioned an investigation into 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 Wbp

61 Cf. Parliamentary Papers 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 view, the AP assumes that Uber has committed the breach of security as referred to

in

Article 13 of the Wbp is not disputed.

64 Report [CONFIDENTIAL] dated January 10, 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 persons have deleted a total of 16 files from the AWS S3 storage

of the Uber group65 and thus had access to and knowledge

of the data contained therein. According to the unauthorized, they were able to access the so-called

get Uber's private GitHub repository 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 lasted almost five weeks.

During that period, in any case, these unauthorized persons could gain access to personal data of

Uber customers. This included unencrypted personal data such as first name,

surname, email address and phone numbers of Dutch Uber users.68 Uber disputed

not that there was a breach of security. This constituted an infringement

to 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 backups of the databases

downloaded by the unauthorized. This shows that, among other things, first name, last name, e-mail address and

phone numbers of Dutch Uber users in the downloaded database backup present

were.69

3.3.4

Pursuant to Article 34a(1) of the Wbp, there is first a notifiable breach of the

security if that breach "results in the significant potential for serious adverse consequences or serious adverse"

consequences for the protection of personal data.

Because in this case, unauthorized persons downloaded files from Uber on its AWS S3 storage and

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

Uber customers were subject to unlawful processing and the adverse consequences for the

protection of personal data has actually manifested itself. That is why it is judged

of the AP there are serious adverse consequences. It is here in the words of the memorandum of

Infringement has a (significant chance of) serious adverse consequences

65 Cf. the findings of [CONFIDENTIAL] as recorded in its report on p. 4 and 5. In the letter dated 22 October 2018

sent addendum belonging to the report of January 10, 2018 as a result of 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. e-mail conversation on November 15, 2016 between 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 [CONFIDENTIAL] report.

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 for a 'successful hacker attack', which in itself is an important indication that

there is a notifiable data breach.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-US.71 Furthermore, it 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 further notes that it concerns - as is possible -
are drawn from the survey conducted by [CONFIDENTIAL] - 31 species
personal data, as shown in the paragraph 'facts and procedure'.
The scope 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 to be resold, for example73
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 have 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 concerned, the type of personal data and the fact that they originated
were from customers of one company, which is also active worldwide. As a result, Uber
legally obliged to report the data breach. Uber's argument that of serious adverse effects,
at least the considerable chance of this would not be the case, the AP therefore considers incorrect.
Purely by way of illustration, the AP notes the following in this regard. If Uber actually believed
that she did not have to report 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
is paid out, and has stipulated with them secrecy of the data breach.76 This implies

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

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

72 Cf. annex 4 to Uber 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 where someone receives fake emails that try to direct them to a fake website.
to lure. cf. https://www.rijksoverheid.nl/onderwerpen/cybercrime/vraag-en- Antwoord/phishing. Spear is a form of phishing

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

give a sense of confidence. An e-mail arrives, which appears to be from a reliable source, but in

in reality, it leads the user to a fake website, which is, for example, full of malware. Such a targeted attack is often

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 (Government Gazette 2015, no. 46128). See also:

https://autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-publishers-policy-rules-

duty to report data breaches

76 In this regard, reference is made to what has been considered in this regard in the present decision regarding the serious

culpable negligence.

according to the AP, it is correct that Uber apparently also considers the data breach to be particularly serious and also serious

had an adverse effect on the protection of personal data, at least a significant chance of that

existed. The person reporting 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 considerable chance of) serious adverse consequences, can also be inferred from the fact that the

[CONFIDENTIAL] by UTI before a United States Senate subcommittee.

has defended the higher than normal amount paid to the notifiers and has stated that this is

done with a view to protecting the personal data of Uber's customers.78 In addition,

Uber's CEO publicly publicized the data breach via a statement posted on her

website.79 Various public sources, including the Uber website, have also shown that Uber

a $148 million settlement was recently made in connection with the concealment of this data breach

has struck with the authorities in the United States.80 Also against this background, the AP follows Uber

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

significant chance of this, there would be no question, and Uber would only provide the notification “without obligation and on its own initiative”.

movement' and 'in the context of transparency'.

Other parts of Uber's view and AP response

That the unauthorized persons - until now - have not further disseminated, resold or

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

there was therefore no question of (a considerable 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 (significant chance of) serious adverse consequences. Also the 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 the

The AP does not believe that a data breach such as the present one does not need to be reported. Other than

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

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

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

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 are not sensitive, the data leak is therefore always subject to the

notification obligation

would be changed. 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 Uber's letter of 11

added December 2017).

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

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

80 See, among others: 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-arranged-for-148-million-dollar-after-hugging-data-lek.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 'Reporting obligation for data leaks in the Personal Data Protection Act (Wbp)', p. 2.

the number of data subjects whose personal data has been leaked may be a reason to investigate the data leak report. This is also apparent from the policy rules.82 The above also applies to Uber's statement in its view that the data breach was resolved on November 15, 2016, the unauthorized persons were out for a reward and there was no indication of misuse or potential for misuse of personal data. Also this one circumstances, whatever that may be, do not entail that the present data breach does not was notifiable.

3.3.5 Data breach not reported immediately

In the event of a data breach that is subject to notification, Article 34a(1) of the Wbp obliges the responsible person to inform the supervisor of this 'immediately'. What in a concrete

case should be regarded as ‘immediately’ depends on the circumstances of the case. ratio is that
the controller should be allowed some time to investigate the infringement. The legislator
has left it up to the supervisor to further define the term 'immediately'.83 The AP has
done in the aforementioned policy rules 'Reporting obligation data leaks in the Personal Data Protection Act (Wbp)'
of 8 December 2015.84 The notification of the data breach must - according to paragraph 6 of the policy rules -
without undue delay, and if possible no later than 72 hours after the discovery, be submitted to the AP
done. The main rule is therefore that the report must be made without undue delay, whereby 72 hours
in principle is the ultimate limit. It should also be noted in this regard that a provisional notification
can be done.85 This means that in practice there will not easily be a reason not to
within 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 was notified of a vulnerability in its
data security. After all, on that date, the then [CONFIDENTIAL] of UTI received an e-mail
mail message from a person86 who informed the [CONFIDENTIAL] that he has a major vulnerability in
discovered the data security of the Uber group.87On November 15, 2016, documents containing
the relevant personal data, downloaded and could be viewed.88 The . notes, for example,
unauthorized in the email correspondence to Uber at “(…) ALL INTERNAL data was able to be downloaded and
seen (…)” and “(…)[CONFIDENTIAL] (…)”. On November 15, 2016, the [CONFIDENTIAL] of UTI
ordered to change passcodes to Uber's AWS S3 storage.89 Based on the information
regarding the infringement which was therefore already at the disposal of UTI 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 what personal data is involved. If necessary, the notification
can then be

be supplemented or withdrawn. cf. paragraph 6, p. 31 of the policy rules 'Reporting data breaches in the Protection Act personal data (Wbp).

86 This person used a pseudonymous e-mail address.

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

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

89 Cf. e-mail conversation on November 15, 2016 (more specifically, the e-mail to the reporter dated November 15, 2016 at 9:29 AM), which as

Appendix 3 to Uber's letter dated December 11, 2017.

Date

Nov 6, 2018

Our reference

[CONFIDENTIAL]

In view of the foregoing, the AP is of the opinion that UTI had already reasonably reported on 15 November 2016 can and should make of the data breach, because a report after that moment, in view of the above mentioned circumstances, in the opinion of the AP, can be qualified as an 'unnecessary' delay" as referred to in the policy rules. But in any case, the report had to be received within 72 hours after 14 November 2016 - the day Uber was notified of the data breach - should take place. This had should also reasonably be done if the exact extent of the data breach is not yet known at that time was known or could not yet be assessed. After all, as said, a provisional notification could also be made done.

UBV reported the data breach to the AP on 21 November 2017 by means of the website of the UBV AP made available web form. The period for reporting the data breach begins, according to aforementioned policies:

"to run the moment you, or a processor you have engaged, become aware of an incident that may fall under the data breach notification obligation."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 on November 14, 2016
to report to the AP. The data breach was first reported on November 21, 2017 and thus 371
days after its discovery, thus exceeding the prescribed period of 72 hours
exceeded. An immediate notification as referred to in Article 34a(1) of the Wbp is therefore
no way. In addition, the AP notes that, now that UBV has submitted the data breach to the AP on November 21, 2017
reported, the AP considers this report to have been made partly 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 the processor becomes aware of the incident - and to the extent that UTI
this context should be considered a processor - Uber cannot hide behind the
the circumstance that UTI as processor has merely failed to fulfill its obligations under private law
towards UBV, as it puts forward in its view.

Completely superfluously, the AP also notes that also in the case of UBV as the (only)
should be regarded as responsible, or if UBV – as a joint
responsible person with UTI – can legitimately rely on the fact that they can only be charged by UTI at a later time
has been informed of the data breach, the notification on November 21, 2017 by UBV to the AP is still
has not been made 'immediately' after becoming acquainted with UBV. UBV is in the person of the [CONFIDENTIAL]
after all, on October 25, 2017, became aware 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.”91 In the judgment
of the AP, UBV cannot legitimately invoke ignorance, which consists in the fact that the

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

91 Appendix 1 to Uber's written opinion of 3 July 2018.

Date

Nov 6, 2018

Our reference

[CONFIDENTIAL]

[CONFIDENTIAL] of 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 - an IT . on 25 October 2017,
security incident that could cause potential media attention - in the opinion of the AP
reasonably in his way to critically inquire in order to find out whether there was any
a data breach, or whether personal data was involved and what the relevance of the 'IT security incident' was
was for UBV. And even if it must be assumed that UBV will enter into force on 10 November 2017 for the first time,
would have been notified of the data breach, as Uber argues,93 then there is still a wide
exceeding the prescribed period of 72 hours, nor is an immediate report
talk.94
The importance of an immediate report, as already explained above, lies in, among other things, the
maintaining and restoring public, customer and regulatory trust in Uber. A
immediate reporting enables the DPA to form its own picture of the facts in a timely manner, to form an opinion
be able to provide information about the measures taken and, under certain circumstances, confidentially with the
be able to consult with the responsible person and intervene if necessary.95 Because in this case the
the prescribed period of 72 hours has been amply exceeded and therefore an immediate notification
of the data breach, there is a situation in which that trust in high
mate is ashamed. In this regard, it is emphasized once again that a data breach can also be subject to certain conditions
reported and can be supplemented or withdrawn if necessary.

Uber view and AP response

Uber's explanation for failing to report to the AP within the 72-hour period
data breach was marked in the research report as insufficiently motivated. Uber has indicated that
has not been reported in time, but that it cannot explain why this has not happened.96 Uber's position in
her view in which she indicates that after being informed by UTI of the data breach, UBV
still reported the data breach to the AP within an 'adequate' term on November 21, 2017 (and through its

authorized representative on November 20 announced the intention to report to the AP) convinces

the AP does not. As noted, (also) UTI, as (jointly) responsible on November 15, 2016, had

at least in any case no later than 72 hours after UTI became aware of the data breach on November 14, 2016

can and must report the data breach.

In its view, Uber further states that the notification form was not made for foreign countries

companies and is specifically aimed at Dutch companies. In this regard, the AP notes

that it cannot be concluded from this that this would dismiss UTI, as jointly responsible

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

UTI could have contacted AP about this. The AP also remarks unnecessarily that

92 Ditto.

93 This date is stated in paragraph 5.26, p. 37 of Uber's view is not in dispute in any way as the date on which 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 because the

data breach

had already occurred in 2016.

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

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

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

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

can appoint an authorized representative in the Netherlands.

3.3.6 Conclusion

From the above, the AP concludes that UBV and UTI, as (joint) responsible parties 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(1) of the Wbp, the data breach was/were obliged to report to the AP. However, the notification to the AP first 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 should be assuming that - in the interpretation of Uber - only UBV is responsible and UTI processor, this assumption does not lead to a different conclusion, now that the 72-hour period based on the policy rules runs from the moment the processor (UTI in this case) becomes aware of the incident, at know November 14, 2016.

3.4

Violation of the obligation to report to the person concerned

Introduction

Infringement is likely to adversely affect 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 an obligation to report data breaches to the data subjects. Pursuant to this reporting obligation, the responsible party must: notify the data subject without undue delay of a security breach if the breach is likely will have an adverse effect on his privacy. Both UBV and UTI are, as jointly responsible person, standard addressee. For the sake of brevity, the AP refers in this regard to what has already been considered above about the violation of the obligation to report to the AP. The same applies at regarding the security breach.

3.4.2

Pursuant to Article 34a, second paragraph, of the Wbp, there is a reportable infringement if the infringement is likely to have adverse consequences for the privacy of the data subject(s) who concerns. Because in this case, unauthorized users have files from Uber from its AWS S3 storage

downloaded and thereby had access to, and knowledge of, the information contained therein

In the opinion of the AP, personal data of Uber customers has unfavorable consequences for the

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

of the scope of the concept of personal privacy, that personal data are

protected as a 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

Nov 6, 2018

Our reference

[CONFIDENTIAL]

In addition to the fact that unauthorized persons had access to Uber's storage – and therefore to the data contained therein

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

personal data98, 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 that the (probable) unfavorable consequences are all the more likely. Due to this combination of

factors, the dataset becomes extra attractive to be resold, for example,99 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 unfavorable consequences, such as the risk of, for example, (spear) phishing. At that time it was

a real risk and could not reasonably be excluded.

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

Wbp, was obliged to report the data breach to the data subjects concerned. In this regard, the
AP also notes that it has not been stated or shown that a situation as referred to in Article 43 occurs
Wbp and on the basis of which the responsible party does not comply with the reporting obligation from Article 34a, second paragraph, Wbp
can be applied.

3.4.3 Data breach not (immediately) reported

The AP has established that the data breach was not reported to the data subjects and therefore there was no question of an immediate notification, as required by Article 34a, second paragraph, of the Wbp. What in a specific case should be regarded as immediate will depend on the circumstances of the case. In the several times the aforementioned policy rules on data breaches, the AP indicates that reporting without delay means that after the discovering the data breach, some time may be taken for further investigation so that those involved can be informed in a proper and careful manner by the person responsible. From the policy rules also show that, just as with the notification to the DPA, it is possible to choose to to inform those involved in the first instance on the basis of the information that is being so that those involved can take measures in advance. A 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 regarding 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 made. The AP believes that Uber, counted from November 14, 2016 at the latest within 72 hours, and in line

98 It has already been stated above in this Decree in the case of the violation of the obligation to report to the AP that this concerns data from 57,383,315 Uber
users, including 25,606,182 US and 31,777,133 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 where someone receives fake emails that try to lead them to a fake website. to lure. cf. https://www.rijksoverheid.nl/onderwerpen/cybercrime/vraag-en- Antwoord/phishing. Spear is a form of phishing

phishing. The personal data (name, e-mail address, telephone number) of the victim is used to give him a give a sense of confidence. An e-mail arrives, which appears to be from a reliable source, but in in reality, it leads the user to a fake website, which is, for example, full of malware. Such a targeted attack is often more successful than a general phishing campaign.

101 See p. 45 of the data breach policies.

Date

Nov 6, 2018

Our reference

[CONFIDENTIAL]

with what the AP has considered with regard to the obligation to report to the AP, inform the parties involved should and could have said 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(5) of the Wbp, the notification to the data subject is made in such done in such a way that, taking into account the nature of the infringement, the established and actual consequences thereof 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 data subjects 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 email. By far the most cases, the controller will have contact details of the data subjects and can stakeholders are also individually informed. In the case of more extensive incidents, a combination of general and individual disclosures are appropriate, such as a notice on the company website and an individual email to affected customers. The important thing is that so many possible data subjects are reached and informed about the consequences to be encountered by him or her measures to limit the consequences for privacy as much as possible. With just one report in the media, that goal is not achieved.103 In the opinion of the AP, in view of the

Uber available contact details to approach the affected Uber customers individually and
only a statement in a press release was not sufficient.

3.4.5

In its view, Uber states that the data breach did not have to be reported to data subjects because there
various technical and organizational security measures have been taken. In this regard
the AP notes that the security measures taken by Uber were aimed at preventing the data breach
close and prevent repetition. However, this does not mean that it should be concluded from this that
during the period of the infringement there was no situation that the infringement is likely
will have unfavorable consequences. As explained above, the AP is of the opinion that there is a
infringement likely to have unfavorable consequences. Also, the Uber-affected
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 - after all, at the time of the leak, they were unprotected (unencrypted) and accessible to
and in the possession of unauthorized persons. As mentioned, the measures to which Uber refers were subsequently
implemented
taken to stop the leak and prevent recurrence.
Uber further states that the data breach was unlikely to have any adverse consequences
because it is not sensitive data.

Uber view and AP response

102 Cf. p. 43 of the policy rules on data breaches 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 should be assumed that the data breach must not only be reported to the AP, but also to those involved.104 It is with other words a very important indication that a notification should be made to data subjects. Based upon of the policy rules it appears that in all other cases the responsible party, on the basis of the circumstances of the case must be considered. The circumstance that a data breach is not refers to sensitive data, does not mean that a notification to data subjects can therefore be omitted stay. In this case, there were sufficient reasons that led Uber to commit the data breach to report those involved.

Uber further argues in its view that there is no evidence that more than two individuals have had access to the relevant personal data for a short period of time, that Uber login data became unusable and introduced two-factor authentication. According to Uber, everything indicates that the unauthorized persons have deleted the downloaded files without sharing them with others. Uber has non-disclosure agreements with the unauthorized parties and knows their identities. That determined personal data were available for two individuals for a short period of time, according to Uber does not make it likely that the personal data concerned (names, e-mail addresses, telephone numbers) for spam or phishing are used, not to mention whether this could be seen as a violation 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 deleted, they have signed a nondisclosure agreement and have disclosed their identity, and according to Uber, it is unlikely that the personal data in question is for spam or phishing 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 posed a significant risk of further spread. Incidentally, this also

At the moment it cannot be ruled out that the data in question is not still available somewhere - outside of Uber - to be. The data breach lasted for five weeks. During that period, the unauthorized access to the relevant personal data without Uber's influence. That has, like

set out above, involves risks. In the opinion of the AP

sufficient reason to conclude that the data breach had been reported pursuant to Article 34a(2) of the Wbp

should be made available to those involved.

Finally, in its view, Uber states that 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 data subject - was allowed to open it

that the AP also believes that it is unlikely that the data breach could have unfavorable consequences for the

involved.

The AP does not follow Uber in its argument. To this end, the AP first of all notes 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

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

Seriously culpable negligence

AP.105 That assessment must be made when the data breach was known to Uber. That

was already on November 14, 2016. As explained with reasons above, there was then sufficient reason to

data subjects to report the data breach. In retrospect, it has not yet become apparent

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 foregoing, the AP concludes that UBV and UTI, as jointly responsible parties,

wrongly and in violation of Article 34a, second paragraph, of the Wbp, have not immediately notified

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 concluded that UBV and UTI are jointly responsible within the meaning 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 under Article 34a, first and second paragraph, of the Wbp. Failure of a timely reporting the data breach to the AP and timely notification of those involved is, in the opinion of the AP resulted from grossly culpable negligence. The AP then motivates that position. To that end she will first of all, explain the legal framework and outline what knowledge a standard addressee considers it to be is to have. Next, the AP will inform the Uber group's science about the seriousness of the data breach judge. Thereafter, the AP will indicate facts and circumstances that, in the opinion of the AP, make that failure to timely report the data breach to the AP and timely notification of data subjects is the result of grossly culpable negligence.

3.5.2 Legal framework

At the time of the violation, Article 66, paragraphs 3 and 4, 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 provisions of Article 66, second paragraph, the articles referred to, then after it has issued a binding instruction. The College can de set a time limit for the offender within which the instruction must be complied with.

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

4.

(…)”

According to the parliamentary history of 'serious culpable negligence' as referred to in Article 66,

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

105 Cf. p. 39 of the data breach policies

Date

Nov 6, 2018

Our reference

[CONFIDENTIAL]

is the result of gross, considerably careless, negligent or injudicious act.”106 In this regard

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 are

mentioned examples of data breaches 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 details and

a company is confronted with 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 (illegible) passwords. However, it is possible that certain

passwords can be retrieved. 108

The Policy Rules on the obligation to report data breaches also addresses the question of when a data breach must be

reported

be reported to the AP. According to Article 34a, first paragraph, of the Wbp, this must be done “immediately”.

In the Policy Rules on the obligation to report data breaches, the AP has specified the term “immediately”.

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(1) of the Wbp).

Reporting without delay means that, after discovering a possible data breach, you may take some time for
further investigation in order to avoid an unnecessary report.
What should be regarded as 'immediately' in a specific case will depend on the circumstances of the
the case. Below you will find the principles that the Dutch Data Protection Authority has with a view to:
has 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, notify the
Dutch Data Protection Authority, unless your investigation has already shown at that time that the incident
does not fall under the data breach notification obligation. If you report the incident later than 72 hours after discovery,
supervisor, you can provide reasons, if requested, as to why you made the report later.
You may not have a full view of what happened and for what reason 72 hours after discovering the incident
personal data it concerns. In that case, you make the report based on the data you have at that time
has. If necessary, you can add to or withdraw the notification later.
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
Nov 6, 2018
Our reference
[CONFIDENTIAL]
In order to be able to report data leaks in a timely manner, you will have to make good agreements with the processors you
may need

so that they provide you with timely and adequate information about all relevant incidents."

The AP assesses the knowledge that a standard addressee (UBV and UTI jointly) of the

applicable laws and regulations is deemed to have taken on the basis of

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

The AP has also amply informed market parties about the applicable laws and regulations, so that

it can be assumed that Uber was also aware of this. In addition, extensive attention has been paid in the media

spent on the obligation to report data breaches.

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

obligation to report data breaches, which Uber could have taken cognizance of before the data breach, follows to the

In the opinion of the AP it is sufficiently clear that Uber had informed the data breach of both the data subjects and the AP

must report and that this immediately, but in any case no later than 72 hours after the discovery on 14

should have happened in November 2016. Moreover, the report to the AP could have been conditional

be made, in the sense that the notification could be supplemented at a later date. That possibility

is expressly provided for in the policy rule.

If doubt had arisen about the scope of the commandment, then, also according to settled case law,

apply that a professional and multinationally operating market party such as Uber may be required

that it properly informs itself or has itself informed about the restrictions to which its behavior is subject

subject, so that she could have aligned her behavior from the outset to the scope of that

commandment.110

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

In the opinion of the AP, UTI management was aware of the seriousness of the data breach. Such

is apparent in the first place 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.

This is also apparent from the additional agreements, which are otherwise customary, that

the reporters have been closed with the intention to keep the data breach secret. The AP explains this as follows.

3.5.3.1 Speed of payment agreement

On Monday, November 14, 2016, UTI was notified of a vulnerability in its

data security. After all, on that date, the then [CONFIDENTIAL] of UTI received an e-mail

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

data security of the Uber group.111 On the same day, the reporter informed UTI

announced 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 January 25, 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 September 19, 2016, ECLI:NL:CBB:2016:290, r.o. 8.6., CBb 19

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

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

Date

Nov 6, 2018

Our reference

[CONFIDENTIAL]

On Tuesday 15 November 2016, the reporter leaves the contact with the reporter to the [CONFIDENTIAL]

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.”

On November 15, 2016, the [CONFIDENTIAL] asked 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 password. 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
The [CONFIDENTIAL] of UTI has on Tuesday 22 November 2016 a copy of the agreement with
the reporters were forwarded.113 When requested, the UTI employee confirmed to the reporters
that the payout 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 the same day that he had received the bitcoins.115 On Thursday, December 15, 2016 is still
once sent an amount of 64.02 BTC to the same address.
E-mail exchanges also indicate 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 normal
reporting a vulnerability is paid for by the Uber group. Unlike Uber sets
its view, in the opinion of the AP this is also a strong indication that UTI was aware
of the seriousness of the data breach. A different explanation for paying a significantly higher
amount than usual Uber did not give. Despite the payment being made through HackerOne,
has notified Uber that the payment was not made as part of the regular Bug Bounty
112 Appendix 3 to Uber's letter of 11 December 2017, as well as the appendix to Uber's additional written response of 21
February 2018.
113 This e-mail is attached to Uber's letter of 21 February 2018.
114 The request and confirmation are attached as Annex 3 to Uber's letter of 11 December 2017.
115 See the email attached as Appendix 3 to Uber's letter of 11 December 2017.

116 That e-mail is attached to Uber's letter of 21 February 2018.

Date

Nov 6, 2018

Our reference

[CONFIDENTIAL]

program of Uber.117 In the opinion of the AP, Uber has deliberately changed this report

treated than other reports of vulnerabilities.

The Uber group's HackerOne page states that the highest bug bounty is in a bandwidth

up to a maximum of $20,000. At the time of the data breach, there was a typical maximum of $10,000,118 De

reporters have expressed a desire for a “6 digits” bug bounty for sharing the found

leak.119 Although the $100,000 bug bounty paid through HackerOne in $10,000 tranches,

exceeds the limit of the indicated bandwidth, Uber declares that the amount to be paid out

bug bounties is subject to the discretion of the Uber group.

On February 6, 2018, UTI's [CONFIDENTIAL] in a subcommittee hearing

of the United States Senate. stated that the payment has the character of a “ransom” for the

removing the leaked data had: “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 the use of 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 payment of $100,000 was agreed, which

is substantially higher than usual, and the subsequent statement of the [CONFIDENTIAL], it appears

in the opinion of the AP that the management of UTI was aware of the seriousness of the data breach at

at the time of that decision-making, and therefore felt compelled to provide the reporting persons with the requested

amount to avoid further harm to Uber users.

3.5.3.3 Confidentiality

That UTI 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 apparent from the additional agreements concluded with the reporters with the intention of keeping the data breach secret at least with the intention of avoiding disclosure.

Confidentiality obligations and obligations to delete research data and no further are not uncommon when reporting vulnerabilities to organizations and businesses, also known as "responsible disclosure". However, not all bug bounty programs require complete secrecy of the research, some organizations make the findings of the researchers public.

At the time of the data breach, the Uber group's policy in its HackerOne bug bounty program was that researchers were allowed to publish about the vulnerabilities they discovered after the vulnerability

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

118 Ditto.

119 That email was attached to Uber's letter of 22 December 2017.

120 See annex to Uber's letter of 7 February 2018.

was resolved by the Uber group. Some of the Uber group's fixes via HackerOne vulnerabilities have been published by the Uber group itself. The Uber group has announced 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 via the bug bounty program.121

In the present case, however, UTI has entered into additional agreements with the reporters, which forbade the reporters to come forward in any way with the discovered data breach. This additional agreement complemented the Uber group's policy for HackerOne, and exhaustively regulated the agreement between the reporters and UTI where conflicts between the standard policy of the Uber group and the agreement in question existed. A provision regarding confidentiality is included in the agreement governing the payment of the bug bounty. In this agreement provides that “[researchers] have not and will not disclose anything about the vulnerabilities or your dialogue with us to anyone for any purpose without [UTI’s.] 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 personnel shows that secrecy of the data breach by the reporters is considered essential by UTI. Commenting on a document about the handling of the data breach, the following is written: “ensuring that the research isn't written about, presented on, etc.”123

Based on the above, the AP finds that UTI's management was aware of the seriousness of the data breach and that she was committed to keeping the data breach secret, at least to to prevent disclosure.

3.5.4 Seriously culpable negligence

As jointly responsible, both UTI and UBV were liable for the entirety of the data processing and the associated 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 do not immediately report the data breach to the AP and those involved. That UBV and UTI have failed to do it reporting a data breach to the AP in a timely manner and informing those involved of the data breach in a timely manner is the result of

acting rudely, considerably carelessly, negligently or injudiciously. In this regard, the AP points out on the following facts and/or circumstances taken together.

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

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

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

123 This quote comes from an email attached to Uber's letter of 10 January 2018.

Date

Nov 6, 2018

Our reference

[CONFIDENTIAL]

e-mail message from a person who informed the [CONFIDENTIAL] that he discovered a major vulnerability in the data security of the Uber group.

Second, as described above, UTI's management was almost immediately, at least shortly after the initial notification aware of the circumstances from which it reasonably follows that the a breach of security leading to the significant potential for serious adverse consequences or has serious adverse consequences for the protection of personal data.

Thirdly, as described above, of a large multinational company as the Uber group may be expected to comply with the legal obligations in the countries in which it operates. The AP assumes that UTI is aware of it was that the obligation to report data leaks, as regulated in Article 34a Wbp, applied to it at the time of the data breach. At the very least, UTI should have known about the obligation.

Referring to the violation section of this decision, the AP is of the opinion that UTI was already 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 committed to the data breach secret, at least to prevent public disclosure, and the data breach was only completed more than a year after discovery of the data breach at UTI on November 21, 2017 reported by UBV to the AP. In the light of the The AP cannot conclude from the above other than that there is serious culpable negligence on on the part of UBV and UTI as jointly responsible.

Even if Uber should be followed in its argument that only UBV should be responsible and UTI as the processor, then according to the Policy Rules, the obligation to report data leaks still has always apply that the data breach occurred on November 14, 2016, at least no later than 72 hours after the discovery on November 14, 2016.

November 2016, should have been reported to the AP. In the Policy Rules on the obligation to report data breaches, this connection stated 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.” UBV's view that on 4 November 2017 an initial meeting took place between UTI and UBV and that UBV took cognizance for the first time on 10 November 2017 that the downloaded files (also) concerned personal data of Dutch users, does not matter either the above judgment of the AP.

UTI was obligated on the basis of the processor agreement concluded between UTI and UBV on March 31, 2016 “[to] promptly notify Uber B.V. about: (ii) any accidental or unauthorized access.”124 Given the joint responsibility, the group relationship and Policy Rules on the obligation to report data leaks, the UBV can refer to not exculpate the judgment of the AP with the fact that UTI has failed to inform UBV.

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

[CONFIDENTIAL]

Incidentally, the AP notes that the [CONFIDENTIAL] of UBV was informed on 25 October 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 make a legitimate appeal act on ignorance, which consists in the fact that the [CONFIDENTIAL] of UBV does not have a “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 have potential media attention cause - in the opinion of the AP it would have been reasonably in its path to continue critically in order to find out whether there was a data breach, or whether it involved personal data involved and what the relevance of the 'IT security incident' was for UBV. By failing to do so, UBV . has equally seriously culpably negligent.

Even in the event that the AP would go along with UBV's view, namely that on November 10, 2017, is the first to take cognizance of the downloaded files with personal data from Dutch users and therefore should have reported it to the AP no later than 72 hours after that knowledge, the AP has established that UBV reported the data breach well too late with its notification on November 21, 2017.

The AP also finds that UTI and UBV have wrongly failed to inform those involved without delay in the prescribed manner of the data breach.

The AP sees no reason for the other circumstances presented 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, it appears from all of the above that UTI and UBV grossly, considerably carelessly, have acted negligently or injudiciously, resulting in serious culpable negligence on the part of UBV and UTI.

4.

4.1

As noted in the previous paragraph, with regard to the amount of the fine, the AP will

the offender can apply the most favorable provision by joining the penalty regime of the Wbp. In the

In the following, the AP will first briefly explain the penalty system, followed by the determination of the

fine in the present 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 Criminal Code, the

maximum of the fine of the sixth category as of 1 January 2016: €820,000.

125 Appendix 1 to Uber's written opinion of 3 July 2018.

126 Ditto.

Amount of the fine

The System

Introduction

Date

Nov 6, 2018

Our reference

[CONFIDENTIAL]

The AP has established 'Fine Policy Rules for the Dutch Data Protection Authority 2016' (Fine Policy Rules)

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

of the amount thereof.127 In the Fine Policy Rules, a choice has been made for a category classification and bandwidth

systematically.

The finable provisions on compliance with which the AP monitors are per statutory maximum fine

of €820,000, €450,000 or €20,500 classified into a number of fine categories, and associated with them in

height of increasing fine bandwidths.

The fine categories are ranked according to the seriousness of the violation of the aforementioned articles,

where category I contains the least serious violations and category II or III the most serious violations.

Violation of Article 34a, first paragraph, Wbp and violation of Article 34a, second paragraph, Wbp are both

classified in category II.

The AP sets a basic fine within the bandwidth. The basic principle is that the AP will pay the basic fine

sets 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 decreasing or increasing the base amount. In principle, within the

bandwidth of the fine category linked to that violation. It's a review

of the seriousness of the violation in the specific case, the extent to which the violation to the offender

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

circumstances of the offender. The AP can, if necessary and depending on the extent

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

apply penalty bandwidth of the next higher and next lower category respectively.

4.3

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

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

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

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

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

Seriousness of the violation

According to article 6, first paragraph, of the Policy Rules, the DPA takes the seriousness of the violation into account. Bee

In assessing the seriousness of the violation, the AP takes into account, among other things, the nature and extent of the

The category classification 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

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

128 Penalty Policy Rules, p. 10-11.

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

company.129

Pursuant to Article 34a(1) of the Wbp, as that provision applied at the time of the violation, the

the responsible person to immediately notify the AP of a security breach, as referred to in

Article 13 Wbp, which leads to the considerable chance of serious adverse consequences or serious adverse consequences

consequences for the protection of personal data.

Pursuant to Article 34a, second paragraph, of the Wbp, as that provision applied at the time of the violation, the

the person responsible to inform the data subjects without delay of a security breach, if

the infringement is likely to adversely affect his privacy.

The purpose of the notification obligation is to prevent data leaks and, if they do occur, the consequences

for those involved as much as possible. The notification obligation contributes to the

maintaining and restoring trust in the handling of personal data.130

Transparency about the nature of the data breach, its probable scope and nature of the potential

damage, the efforts made to repair the damage and advice to the public and

customers to enable themselves as best as possible to avoid the consequences for their own interests

oversight are necessary measures to maintain and restore that trust. That trust

is supported by the need to enable the AP to form its own image of the

facts, be able to express an opinion about the measures taken, in circumstances confidential with

be able to consult with the person responsible and intervene if necessary.131

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

In the period from November 15, 2016 to at least November 21, 2017, UBV and UTI have failed to to inform the data subjects without delay of the data breach. Only on November 21, 2017, UTI has the stakeholders informed by means of a news item. As a result, those involved are not (timely) able to to oversee the consequences for its own interests by, for example, being alert to the risk of (spear) fishing. In addition, the data subjects do not have, or at least did not have in a timely manner, can take precautionary measures to mitigate potentially adverse consequences of the data breach. This considers the AP serious.

When assessing the seriousness of not reporting the data breach without delay, the AP also has the size of the data breach. 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 should give cause to notify 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 also in line with the criterion from Article 83(2)(a) of the 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 had, or at least could have had. In the opinion of the AP,

the violation seriously harmed confidence in the handling of personal data.

In addition, UBV and UTI at least 72 hours after the discovery of the data breach on November 14, 2016, until November 21, 2017, failed to notify the AP of the security breach. Thus is the AP was not aware of the (extensive) data breach for a longer period of time. the AP has therefore not been able to form its own picture (in time) of the facts and any possible Uber measures taken, both towards those involved and with regard to the necessary handling of the (acute) vulnerability. Due to this omission of UTI and UBV, the AP has been seriously hampered in its supervision, which indirectly also affects the interests of those involved.

On balance, the AP sees reason to change the basic amount of the fine, based on the degree of seriousness of the fine violation, to be increased by one third per violation to €327,845.

Degree of culpability of the offender

According to Article 6, second paragraph, of the Policy Rules, the DPA takes into account the extent to which the offense can be blamed on the offender.132 If the offense was committed intentionally or if it 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 means that 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 breach should be made. Despite this, the Uber group was committed to keeping the data breach secret hold, which Uber has been willing to pay a substantially higher amount of money than usual pay to reporters and agree additional confidentiality obligations with the reporters.

Only more than a year after the discovery of the data breach at UTI was the data breach on November 21, 2017 by UBV reported to the AP and a news story has been 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 change the basic amount of the fine, based on the degree of culpability

increase by one third per violation.

With the previous steps, the fine amounts to € 409,190 per violation, so that the total amount of

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 also in line with the criterion from Article 83, second paragraph, sub b, GDPR.

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

Application of the proportionality principle according to the fine policy rules of the AP, among other things:

play in the accumulation of sanctions. If the AP for distinct, but coherent

If you want 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 will 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 distinct violations. After all, Article 34a,

first paragraph, of the Wbp, requires that the AP is immediately notified 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 purport of the relevant provisions in the core

is equivalent, namely transparency with a view to building trust in the handling of

retain and/or restore personal data. Furthermore, the AP is of the opinion that the conduct

the offenses are based essentially on the same set of facts. This gives

reason to moderate the above-mentioned fine on the basis of proportionality.

In assessing proportionality, the AP also takes into account the fact that, despite the

lapse 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 at € 600,000. Given its financial situation, this amount can be

wearing position.

5.

The AP jointly submits to the UBV and UTI, because of 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

to be.

UBV and/or UTI must transfer the amount to a bank account within six weeks

[CONFIDENTIAL] in the name of the Dutch Data Protection Authority, stating 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 will be suspended until the

objection has been decided. This obligation is also suspended if UBV and/or UTI are in

appeals, until a decision has been made on the appeal.135

dictum

133 Penalty Policy Rules, p. 11.

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

135 See Article 71 Wbp.

Date

Nov 6, 2018

Our reference

[CONFIDENTIAL]

The Dutch Data Protection Authority,

On their behalf,

w.g.

mr. A. Wolfsen

Chair

Remedies Clause

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

decides 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.