Confidential/Registered

National Police

Attn. the Chief of Police

[CONFIDENTIAL]

New Explanation 1

2514 BP THE HAGUE

Date

November 12, 2018

Subject

Load under duress

Our reference

z2018-05664

Contact

[CONFIDENTIAL]

Authority for Personal Data

PO Box 93374, 2509 AJ The Hague

Bezuidenhoutseweg 30, 2594 AV The Hague

T 070 8888 500 - F 070 8888 501

authoritypersonal data.nl

1 Introduction

By decision of February 6, 2017, the Dutch Data Protection Authority (AP) has sent the National Police (NP) a

order subject to periodic penalty payments imposed.1 This order subject to periodic penalty payments consisted of five parts

and related

on the security and training regulations of the national in use by the NP

Second Generation Schengen Information System (N.SIS II). At the end of the beneficiary period

the AP has determined that the NP has complied with four of the five burden components. The AP has

found that the NP did not meet the burden component pertaining to the regular and proactive

checking log files. This left one violation of Section 4(3) of the Act

protection of police data (Wpg), which - as follows from the assessment included in the present Decree -

continues to date.

2. Course of the procedure

The AP has conducted an official investigation into the use of the N.SIS II by the NP. The

research findings are included in the final findings report dated October 22, 2015

(research report).2

As a result of these findings, the AP issued a decision subject to periodic penalty payments on 6 February 2017

imposed, consisting of five parts (I to V). This decision is now irrevocable.

1 With reference z2015-00910.

2 With reference z2015-00126.

Attachment(s): 2

Date

November 12, 2018

Our reference

z2018-05664

After the end of the six-month beneficiary period, the NP sent documents in which it

has made known what measures it has taken in response to the order imposed under

penalty.

By decision of 12 March 2018, the AP determined that the NP was affected by the implementation of the

measures has complied with load components I to IV. 3 The AP has further established that this is not the case

requirement part V has been complied with. Therefore, the DPA in that same decision - which is now irrevocable -

proceeded to collect the forfeited penalty of € 40,000.

In connection with the continuous violation with regard to the aforementioned load component, the AP has added

letter of 29 March 2018 expressed the intention to (again) impose an order subject to periodic penalty payments that extends to take measures with which the NPN will still end the remaining violation.

In a letter dated 11 April 2018, the NP expressed its views on this intention.

A hearing took place on April 12, 2018, at which the NP was given the opportunity to present its views provide oral explanations in writing. The record of the hearing is attached as Annex 1 to this decision attached.

In a letter dated 12 June 2018, the AP requested an explanation of the methods proposed by the NP.

In a letter dated 3 July 2018, the NP provided an additional explanation of its view on request.

In a letter dated 29 August 2018, the NP announced that it had taken measures in this regard of the observed violation.

3. Background

The investigation report established, among other things, that the NP's checks on the log files are generated in the context of data processing in N.SIS II only takes place in the case there are safety signals, integrity investigations, complaints or a technical malfunction.4 Therefore the NP did not comply with Article 4, third paragraph, of the Wpg, which entails that log files from under other events that record user activity should be checked regularly and assessed. The order subject to periodic penalty payments of 6 February 2017 served (among other things) to terminate this offence.

The NP has proposed two approaches – one for the short term and one for the longer term – with which it believes that it can put an end to the violation. Only by letter dated 29 August 2018 did the NP informed the AP that the intended and temporary working method has now been introduced. The AP finds however – with reference to the considerations set out below – that the NP The implemented method does not lead to the termination of the research report and in

3 With reference z2017-10057.

4 See section 3.5 of the research report.

Date

November 12, 2018

Our reference

z2018-05664

the order subject to periodic penalty payments of February 6, 2017 established violation of Article 4, third paragraph, of the Wpg. This is reason for the AP to, pursuant to Article 35, second paragraph, of the Wpg5, in conjunction viewed with Article 58, second paragraph, under d, of the General Data Protection Regulation (GDPR) and Article 16, paragraph 1, of the General Data Protection Regulation Implementation Act (UAVG) and Article 5:32, first paragraph, of the General Administrative Law Act (Awb) to impose the present order subject to a penalty. lay. The order subject to periodic penalty payments is intended to end the aforementioned continuous violation.

4. Explanation of the legal framework

By decision of 12 March 2018, the AP established that the NP has not complied with part V of the order subject to periodic penalty payments of 6 February 2017. The NP has not disputed this. On March 29, 2018, the AP expressed its intention to (again) impose an order subject to periodic penalty payments with regard to the currently remaining, continuous violation. Since then, there have been no material changes to the legal framework occurred that have substantive consequences for the present file.

The legal framework is included as Annex 2 to this Decree.6

5. View of the NP

In letters dated 11 April, 3 July and 29 August 2018, the NP describes two methods with which it believes the violation of Article 4, third paragraph, of the Wpg. It is:

1) a temporary method, [CONFIDENTIAL] and

2) an automatic method that the NP wants to introduce in the longer term [CONFIDENTIAL].7

[CONFIDENTIAL]

5 Article 47 of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons in relation to the processing of personal data by competent authorities for the purposes of prevention,

the investigation, detection and prosecution of criminal offenses or the execution of criminal penalties, and on freedom movement of such data and repealing Council Framework Decision 2008/977/JHA (Directive (EU) 2016/680) refers to the powers of supervisory authorities to take corrective action. This Directive has been implemented in national legislation that has not yet entered into force at the time of this decision. Now the implementation term of this one Directive has expired, national law - including Article 35, second paragraph, of the Wpg - must become directive-compliant interpreted.

6 The aforementioned Directive (EU) 2016/680 requires, among other things, that appropriate technical and organizational measures are taken to ensure a level of security appropriate to the risk. In view of this, an interpretation in conformity with the guideline has no effect material change of the legal framework.

The following applies with regard to the NEN-EN-ISO/IEC 27002:2017 (NEN standard). For the assessment of whether there is appropriate technical and organizational security measures, the AP previously aligned with the further implementation that is given to them the Information Security Code, the NEN-ISO/IEC 27002:2013 standard. It is now in line with the most recent interpretation, namely NEN-EN ISO/IEC 27002:2017. The website https://www.nen.nl/NEN-Shop/Norm/NENENISOIEC-270012017-nl.htm states: 'This European acceptance does not deviate substantively from the NEN-ISO variant with publication date 2013'. The standard has therefore remained materially the same.

Section 12.4 of this document is (particularly) important in the present file.

7 This working method has previously been put forward in the correspondence and documents that the NP has sent to the AP in the context of the inspection by the AP of compliance with load part V of the previously imposed order subject to periodic penalty payments. It is correspondence dated August 4, 2017, November 24, 2017, December 4, 2017, and December 7, 2017.

Date

November 12, 2018

Our reference

z2018-05664

6. Assessment

Pursuant to Article 4(3) of the Wpg, the NP must, in short, provide appropriate, technical and
take organizational measures to protect police data against accidental or
unlawful destruction, alteration, unauthorized disclosure or access. This means that, given the
interpretation given by the NEN standard, log files of events that indicate user activities,
record exceptions and information security events should be made,
kept and regularly reviewed.

[CONFIDENTIAL]

The AP concludes that the NP with the implementation of the temporary and partly manual method
does not regularly and proactively check the log files regarding N.SIS II for illegal activity
processing. This does not provide it with an up-to-date and representative picture of unauthorized access or
unlawful use of police data. In view of the foregoing, the violation of Article 4,
third paragraph of the Wpg.

7. Order subject to periodic penalty payments and grace period

Pursuant to Section 35(2) of the Wpg, viewed in conjunction with Section 58(2)(d),
of the AVG, article 16, first paragraph, of the UAVG and article 5:32, first paragraph, of the Awb, the AP is
the case at hand is authorized to impose an order subject to periodic penalty payments.

The AP attaches a grace period of twelve weeks to the order subject to periodic penalty payments. At the
setting this term, it considered it important that this violation already occurred in October 2015
and has therefore continued for at least three years. The AP also considers it important that
the NP stated at the time in its opinion of 12 April 2018 that the timely and manual

working method largely still had to be worked out, but from 1 September at the latest (i.e. slightly more than twenty weeks later) could be operational. This method is now operational, but the AP has concluded that this method is not sufficient to remove the violation.

In determining the penalty, the AP considers it important that the penalty imposed by decision of 6 February 2017 has been determined, before the ANP has proved to be insufficient incentive to (fully) comply with the associated load to meet. The amount of the penalty in that decision amounted to a maximum in total € 200,000 for five violations, therefore € 40,000 per violation. In view of an early termination of the infringement, which has been ongoing for some time, is the periodic penalty payment in the present decision increased and the additional amount to be forfeited increases by every two after the end of the beneficiary period weeks that the burden has not been met.

In view of the foregoing, the AP comes to the following. If the NP does not observe the violation terminates within twelve weeks, it will forfeit for every two at the end of that period of favour weeks that the order has not been complied with a penalty. The AP sets the amount of this penalty for the

fixed at an amount of € 50,000 (in words: fifty thousand euros). After that, the periodic penalty payment will be increased by one every two weeks amount of € 20,000 (in words: twenty thousand euros)8 up to a maximum amount of € 320,000 in total (in words: three hundred and twenty thousand euros).

8 This means that the NP will forfeit € 50,000 if it has not yet reported the violation two weeks after the end of the beneficiary period.

terminated; two weeks afterwards (four weeks after the end of the beneficiary period) she forfeits an additional € 70,000 (in total

€120,000), two weeks later (six weeks after the end of the beneficiary period), she forfeits an additional €90,000 (in total €210,000) and two weeks thereafter (eight weeks after the end of the beneficiary period) she forfeits an additional €110,000 (in total 320,000).

Date

November 12, 2018

Our reference

z2018-05664

8. Operative part

The AP imposes the following order subject to periodic penalty payments on the NP:

The NP must be submitted within twelve weeks of the date and with due observance of this decision in the context of the data processing in N.SIS II to take measures that ensure that the log files are regularly and are proactively monitored for indications of unauthorized access or use of police data.

If the NP does not de

has implemented measures, the NP will forfeit a penalty of € 50,000 (in words: fifty thousand euros) for the first two weeks after the end of the beneficiary period that the order has not been (fully) executed.

After that, the periodic penalty payment will be increased every two weeks by an amount of € 20,000. (in words: twenty thousand euros). The maximum amount to be forfeited is € 320,000 (in words: three hundred and twenty thousand euros).

If the NP wishes to forfeit the penalty immediately after the beneficiary period has expired the AP advises the NP to provide the documents - with which the NP can demonstrate that it complies with the order subject to periodic penalty payments (for example by means of an audit report) - in a timely manner, but no later than four weeks before the end of the beneficiary period to the AP for assessment.

Yours faithfully,

Authority for Personal Data,

For this,

e.g.

Mr. A. Wolfsen

Chair

Attachments

Annex 1 – Report hearing 12 April 2018

Annex 2 – Legal framework

Remedies

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

decision to submit an appeal to the AP, PO Box 93374, 2509 AJ The Hague, stating:

“Awb objection” on the envelope.

Date

November 12, 2018

Our reference

z2018-05664

Annex 1 to the decision of 12 November 2018 with reference z2018-05664

Report hearing 12 April 2018

[CONFIDENTIAL]

Date

November 12, 2018

Our reference

z2018-05664

Legal framework

General Data Protection Regulation (GDPR)

Article 58, second paragraph, under d, of the GDPR

2. Each supervisory authority shall have all of the following corrective powers

measures:

(…)

d) instruct the controller or processor, where appropriate, to specify

way and within a specified period, to bring processing operations in line with the

provisions of this Regulation;

Implementation Act General Data Protection Regulation (UAVG)

Article 16, first paragraph, of the UAVG

1. The Dutch Data Protection Authority may impose an administrative enforcement order to enforce the bee

or obligations imposed by virtue of the regulation or this law.

General Administrative Law Act (Awb)

Article 5:32, first paragraph, of the Awb:

1. An administrative authority authorized to impose an order under administrative coercion may instead

impose an order subject to periodic penalty payments on the offender.

Police Data Act (Wpg)

Article 2, first paragraph, of the Wpg:

1. This law applies to the processing of police data contained in a file or

intended to be included therein.

Article 4, third paragraph, of the Wpg:

3. The responsible party will take appropriate technical and organizational measures to protect police data

secure against accidental or unlawful destruction, against alteration, unauthorized communication or

access, in particular if processing data transmission over a network or making available

via direct automated access, and against all other forms of unlawful processing,

taking into account in particular the risks of the processing and the nature of the data

protect data. These measures guarantee, taking into account the state of the art and

the costs of implementation, an appropriate level of security, given the risks of the processing

and the nature of the police data.

Article 35, first and second paragraph, of the Wpg

Date

November 12, 2018

Our reference

z2018-05664

1. The Dutch Data Protection Authority supervises the processing of police data

in accordance with the provisions laid down by and pursuant to this Act.

2. Articles 51, second paragraph, 60, 61 and 65 of the Personal Data Protection Act are of

similar applications.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the

protection of natural persons with regard to the processing of personal data by

competent authorities for the purposes of the prevention, investigation, detection and prosecution of

criminal offenses or the execution of criminal penalties, and on the free movement of such data and

repealing Council Framework Decision 2008/977/JHA (Directive (EU) 2016/680)

Article 1, first paragraph, of Directive (EU) 2016/680

Subject and objectives

1. This Directive lays down rules for the protection of natural persons

in connection with the processing of personal data by competent authorities for the purpose of the

the prevention, investigation, detection or prosecution of criminal offenses or the execution of

punishments, including protection against and prevention of dangers to the public

safety.

Article 2 of Directive (EU) 2016/680

Scope of application

1. This Directive applies to the processing of personal data by competent authorities

for the purposes of Article 1(1).

2. This Directive shall apply to fully or partially automated, as well as to non-automated

automated processing of personal data contained in a file or intended

to be included in it.

Article 29, first paragraph and second paragraph, under e, of Directive (EU) 2016/680

Security of processing

1. Member States shall require that the controller and the processor, taking into account

with the state of the art, the implementation costs and the nature, scope, context and purposes

of the processing, as well as the risks to rights varying in likelihood and severity

and freedoms of persons, take appropriate technical and organizational measures to

to ensure a risk-appropriate level of security, in particular with regard to the security referred to in Article 10

processing of special categories of personal data.

2. With regard to automated processing, each Member State shall provide that the

controller or the processor, after assessing the risk, takes measures to:

(…)

Date

November 12, 2018

Our reference

z2018-05664

e) ensure that persons authorized to operate an automated processing system

only have access to the personal data to which they have access authorization

('data access control');

Article 47, second paragraph, of Directive (EU) 2016/6809

2. Each Member State shall provide by law that each supervisory authority has effective powers

to take corrective measures, such as:

a) warn the controller or the processor that with the intended processing operations

there is a likelihood of an infringement of the provisions adopted pursuant to this Directive;

b) the controller or the processor orders the processing operations, where appropriate, to be carried out in a more detailed

manner

certain way and within a specified period of time

directive, in particular by ordering the rectification or erasure of data or restriction of processing

in accordance with Article 16;

c) impose a temporary or permanent restriction on processing, including a prohibition on processing.

Regulation (EC) No. 1987/2006 of the European Parliament and of the Council of 20 December 2006

on the establishment, operation and use of the Schengen Information System of the second

generation (SIS II) (hereinafter: the Regulation)

Article 10, first paragraph, under i and k, of the Regulation:

1. Each Member State shall take appropriate measures for its N.SIS II, including the establishment of a

safety plan, so that:

[…]

i) afterwards we can check and determine which personal data, when and by whom

and for what purpose are included in an automated data processing system (control of the

inclusion);

[…]

(k) the effectiveness of the security measures referred to in this paragraph is monitored on an ongoing basis

and with regard to this internal control, the necessary organizational measures are taken to

ensure compliance with the requirements of this Regulation (self-monitoring).

Article 44 of the Regulation:

1. The authorities designated in each Member State to which the powers referred to in Article 28 of Directive

95/46/EC ("national supervisory authorities"), independently monitor the lawfulness of the processing

of SIS II personal data on their territory and the transfer from that territory, and the

exchange and further processing of additional information.

2. National supervisory authorities shall ensure that an audit of the

data processing in N.SIS II is carried out in accordance with international auditing standards.

3. Member States shall ensure that national supervisory authorities have sufficient resources

to fulfill their duties under this Regulation.

9 Article 47 of Directive (EU) 2016/680 pertains to the powers of supervisory authorities to take corrective action

measures. This Directive has been implemented in national legislation that was not yet in force at the time of this decision

trodden. Now that the implementation period of this Directive has expired, national law - including Article 35, second

paragraph,

of the Wpg - to be interpreted in accordance with the guideline.

Date

November 12, 2018

Our reference

z2018-05664

Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use

of the second generation Schengen Information System (SIS II) (hereinafter: the Decision)

Article 10, first paragraph, under i and k, of the Decree

1. Each Member State shall take appropriate measures for its N.SIS II, including a security plan,

so that:

[…]

i) it can subsequently be checked and determined which personal data, when, by whom and for

what purpose are included in an automated data processing system (control of the

inclusion);

[…]

(k) the effectiveness of the security measures referred to in this paragraph is monitored on an ongoing basis

and with regard to this internal control, the necessary organizational measures are taken to

ensure compliance with the requirements of this decree (internal control).

Article 60 of the Decree:

1. Each Member State shall ensure that an independent authority ('national supervisory authority').

monitors the lawfulness of the processing of SIS II personal data on and from its

territory, including the exchange and further processing of additional information.

2. The national supervisory authority shall ensure that an audit of the

data processing in N.SIS II is performed in accordance with international auditing standards.

3. Member States shall ensure that the national supervisory authority has sufficient resources

to fulfill its duties under this Decision.