

□AUTHORITY

PERSONAL DATA

~ - ~ s .• r.

National Police Attn. the Chief of Police

New Explanation 1 2514 BP THE HAGUE

Authority for Personal Data

PO Box 2509 AJ De.' Hsug

Date Our reference Your letter from

Topic

recovery order

Dear Mr Akerboom,

By penalty decision of 6 February 2017 (decision with reference 22015-00910), the Dutch Data Protection Authority (AP), following the ex officio investigation into the use of the second-generation national Schengen information system (N.SIS II) by the National Police ( NP), decided to impose an order subject to periodic penalty payments on the NP on the basis of Article 35, second paragraph of the Police Data Act (Wpg), viewed in conjunction with Article 65 of the Personal Data Protection Act (Wbp) and Article 5:32 , first paragraph, of the General Administrative Law Act (Awb).

The favoring period included in the penalty decision ran until 6 August 2018. After the grace period had expired, the NP sent documents in which the NP indicated the measures it had taken in response to the order subject to a penalty. The AP has assessed these documents and has established that the NP has not fully complied with the order subject to penalty before the end of the beneficiary period. The AP has decided to proceed with collection for an amount of € 40,000 (in words: forty thousand euros).

1

AUTHORITY

PERSONAL DATA

Date Our reference

'2P'???. t 201.S z23 T7-10057

## 1. Course of the procedure

1. Following the AP's official investigation into the use of N.SIS II by the NP, the AP imposed an order subject to a penalty on the NP by penalty decision of 6 February 2017.<sup>1</sup>

On August 30, 2017, the NP contacted the AP by telephone with the request to e-mail the contact details (e-mail address and telephone number) of the AP's staff member to the NP, in order to send the relevant documents. for the investigation into compliance with the order subject to periodic penalty payments. These contact details were sent by the AP to the NP by email dated August 30, 2017.

3. By e-mail dated 10 November 2017, the AP informed the NP that it had not yet received any documents.

4. By e-mail dated November 13, 2017, the NP informed the AP that a written response regarding compliance with the order subject to periodic penalty payments has fallen into disrepair and will still be sent to the AP.

5. In a letter dated 24 November 2017, the NP informed the AP that the NP has taken various measures in response to the penalty decision in order to comply with the order. The NP has sent a number of documents to substantiate this.

6. In a letter dated November 29, 2017, the AP informed the NP that on the basis of the documents sent on November 24, 2017, it is insufficiently apparent that the burden has been (fully) met. In this regard, the AP has given the NP the opportunity to send additional supporting documents.

7. By letter dated 4 December 2017, supplemented by e-mail dated 5 December 2017, the NP sent documents to the AP regarding the measures taken by the NP with regard to data processing in N.SIS II.

8. By e-mail dated 6 December 2017, the AP requested that further documents be sent to show that the NPN fulfilled the burden of proactively checking the N.SIS II log files for indications of unauthorized access or use of police data.

9. By e-mail dated 6 December 2017, also sent by letter dated 7 December 2017, the NP sent the AP further information regarding the proactive checking of the N.SIS II log files.

10. By e-mails dated 31 January, i, 5 and 6 February 2017, the NPO sent further information showing that authorizations before 7 August 2017 are being logged by the NPO.

1 The findings of the official investigation are set out in the final findings report of 22 October 2015 (hereinafter: the investigation report).

AUTHORITY

PERSONAL DATA

Date Our reference

2. The cease and desist order

11. By decision of 6 February 2017, the AP imposed an order subject to a penalty payment on the NP with the following content:

12. Within six months of the date of this decision, the NP must take measures in the context of data processing in NSIS II that result in:

the NP establishes a procedure relating to authorizations for the functional managers of the parties affiliated to NSIS II and the employees of the IND who process data in the context of NSIS II; establish the NP staff profiles defining the roles and responsibilities of persons authorized to access and process personal data in NSIS II;

the NP ensures that a periodic check is carried out on the authorizations granted to the functional managers of the parties affiliated to NSIS II and the employees of the IND; changed authorizations are logged;

the log files are regularly proactively checked for indications of unauthorized access or use of police data.

i.

CO"

IU.

rv.

v.

i.e. If the NP has not implemented the measures no later than six months after the date of this penalty decision, the NP forfeits a penalty of € 12,500 (in words: twelve thousand five hundred euros) for each week that the order has not been (fully) executed up to a maximum of € 200,000 (in words: two hundred thousand euros).

3. Assessment of compliance with the penalty order

14. The AP finds that the NP has not used any legal remedies against the penalty decision of

February 6, 2017 and that the penalty decision has become irrevocable. This means that neither the content of the order

subject to penalty nor the duration of the beneficiary's period are under discussion. It is assessed whether the NP has met the

burden within the beneficiary period. In view of the fact that the order subject to a penalty was imposed by a penalty decision of 6 February 2017, it must be concluded that the last day of the beneficiary period was 6 August 2017.

15. With regard to the various parts of the burden, the AP concludes as follows.

3.1 With regard to part I of the load:

16. The penalty decision stipulates that, in the context of data processing in N.SIS II, the NPN must take measures that lead to the establishment of a procedure relating to authorizations for the functional managers of the N.SIS II connected parties and IND employees who process personal data in the context of N.SIS II.2

17. In letters dated November 24, 2017 and December 4, 2017, the NP has notified in this regard that the Chief Information Security Officer (CISO) of the NP has adopted the Policy on Supervision of Authorizations for Chain Partners on August 2, 2017. This policy document is appended to these letters and describes

2 The requirements that such an authorization procedure must meet follows, among other things, from the NEN standard.

3/8

AUTHORITY

PERSONAL DATA

Date Our reference

12 r'3t. ~ 20' i z2017- i0057

including the procedures and frameworks with which the authorization of chain partners (including functional managers) functions and how the supervision thereof is organised. The policy document stipulates that the policy will come into effect immediately (on 2 August 2017).

18. In view of the foregoing, the AP establishes that the NP has complied with part I of the burden in a timely manner by adopting this policy on 2 August 2017.

3.2 With regard to part II of the load:

The penalty decision stipulates that, in the context of data processing in N.SIS II, the NPN must take measures that lead to the NPN establishing personnel profiles that describe the tasks and responsibilities of persons authorized to process personal data in N.SIS II. to view and process. The preparation of personnel profiles serves, among other things, as a means of assessing whether the authorizations have been arranged correctly.

20. By letter dated December 4, 2017, the NPN notified that the NPN is introducing a new national authorization model, which defines the personnel profiles and describes the tasks and responsibilities of the persons authorized to use different information systems and process data. A national Identity and Access Management system (IAM) is used for this, which determines which national applications and information will be given access to based on the combination of the person's position and the department where he or she works. To substantiate this, the NP has added the "Police Authorization Model Implementation Plan" as an appendix. dated 26 September 2016. In addition, the NP pointed out that the NP has connected the Schengen Muteer Client (SMC), the system with which users can process data in N.SIS II, to the IAM facility and the national authorization model. As proof of this, the NP has appended the authorization profiles of the Regional Information Organization Service, in which the SMC authorizations are also included, and the application form that must be completed for SMC authorizations is attached. From the intranet message that the NP also sent as an attachment to the letter from 4 December 2017, it appears that the NP has internally announced the transition from the SMC to the national authorization system as of 1 August 2017.

21. In view of the foregoing, the AP establishes that the NP has complied with part II of the order on time.

3.3 With regard to part III of the load:

22. The penalty decision stipulates that, in the context of data processing in N.SIS II, the NPN must take measures that result in a periodic check being carried out on the authorizations granted to the functional managers of the N.SIS. II affiliated parties and the employees of the IND.

23. In a letter dated 4 December 2017, the NP referred to the policy on Supervision of Authorizations for Chain Partners of August 2, 2017, in which an annual check on authorizations is prescribed. In this regard, it was stated that with regard to N.SIS II no check has yet been carried out on the authorizations granted to IND employees, but that a check has now been carried out at the Royal Netherlands Marechaussee.

19.

CD

4/8

AUTHORITY

PERSONAL DATA

Date Our reference

'2 i'-r.r. t 2?'-? z2C'7-1003"

(KMar) and that the periodic investigation into the authorizations of IND employees is planned for the second quarter of 2018.

24. In view of the Policy on Supervision of Authorizations for Chain Partners of 2 August 2017, the AP has established that the NP has taken measures within the beneficiary period that lead to a periodic (annual) check being carried out on the authorizations granted to the functional managers of the parties affiliated to N.SIS II and the employees of the IND. The AP sees no indications that action will not be taken in accordance with this policy.

25. In view of the above, the AP determines that the NP has complied with part III of the order on time.

co

3.4 With regard to part IV of the load:

26. The penalty decision stipulates that the NPN must take measures in the context of data processing in N.SIS II that lead to changed authorizations being logged.

27. By letter dated 4 December 2017, the NP notified that changed authorizations are logged in the generic LAM tool - to which N.SIS II is connected for its authorizations. The NP also explained that since 1 October 2016, the IAM tooling offers the possibility to actively monitor and supervise the use of applications. As an explanation of this, the NP has referred to the attached document Implementation of the Police Authorization Model of 26 September 2016 and the also attached document the LAM monitoring & control process description of 9 January 2017. The NP has explained that different functions are available for the logging of N.SIS II authorizations. are configured. Reference has been made in this regard to the function of keeping a time-trace of the authorization that someone has received via IAM. To illustrate this, the POI has included a configuration file from which it can be deduced which data from the authorization process is stored in the history log. In addition, an example report of the authorization history per employee was sent as an attachment with an email dated December 5, 2017, which provides an overview of all authorization changes that have been made for an employee.

28. By e-mails of 31 January, 1.5 and 6 February 2017, the NPO sent further information showing that changed authorizations were already logged by the PO in 2016 and will also be logged after August 6, 2017. The AP notes that the AP was not previously informed by the NP that changed authorizations were already logged in 2016, while this would have been on the way of the NP.<sup>3</sup>

29. In view of the foregoing, the AP concludes that the NP had already taken measures before the penalty decision as referred to in part IV of the order and that this part of the order has therefore been complied with.

3 The NP has even stated that it will not contest the conclusion from the investigation report, which states that the NP does not log changed authorizations (see penalty decision under paragraph 42). The NP also did not object to the penalty decision, in which this conclusion was reached.

5/8

AUTHORITY

PERSONAL DATA

Date

12 ~ 2:;1 o

Our reference

z20.7-';5"

3.5 Part V of the load:

30. The penalty decision stipulates that the NPN must take measures in the context of data processing in N.SIS II that lead to the log files being regularly proactively checked for indications of unauthorized access or use of police data.

31. In a letter dated 4 December 2017, the NP notified that N.SIS II is connected to the management reporting tool Cognos, with which the responsible managers can check the log files for irregularities. In addition, it has been reported that N.SIS II will be connected to the Security Information & Event Management (SIEM) tooling of the Security Operations and Control Center (SOC). In the attached memo N.SIS II in SIEM dated August 4, 2017, the expectation was expressed that the addition of N.SIS II logging to the SIEM tooling would be realized in September 2017. The SIEM tooling provides automated analysis and monitoring of logging anomalies.

32. The NP explained that in the context of data processing in N.SIS II, the log files are not (yet) proactively checked for indications of unauthorized access or use of police data. In that regard, the NP states that this proactive control is only possible if the central works council (COR) has agreed to this.

33. Whatever else this claim of the NP may be, it does not alter the conclusion that part V of the charge is not being complied with. For the sake of completeness, the AP also points out that the NP could have submitted a reasoned request to the AP for

an extension of the beneficiary period. In addition, the NP could have objected to the favoring period included in the penalty decision.\*

The NP did not make use of either option.

34. In view of the above, the AP determines that the NP has not complied with part V of the order.

#### 4. The penalty payment

35. The penalty decision stipulates that if the NP has not implemented the measures no later than six months after the date of this penalty decision, the NP forfeits a penalty of € 12,500 for each week that the order has not been (fully) carried out until a maximum of € 200,000.--.

36. In view of the fact that the authorization period ran until 6 August 2017, the AP finds that penalty payments were forfeited by operation of law on 14 August 2017<sup>4 5</sup> because the NP did not comply with part V of the order. The maximum amount of forfeited penalty payments has been reached on

4 Incidentally, when determining the beneficiary term, the expectation of the NP that the proactive monitoring of logging could be started in July 2017 was taken into account (see the adopted report of the conversation between the AP and the NP of October 4, 2016).

5 Forfeiture takes place at the end of the time unit of one week after the beneficiary period. See ABRS December 12, 2012 ECLI:NL:RVS:2012:BY5884 and ABRS November 6, 2013, ECLI:NL:RVS:2013:1829.

6/8

AUTHORITY

PERSONAL DATA

Date

Our reference

November 26, 2017. Now that the AP has not paid the five parts of the order in only one part, the AP has decided to proceed to collect the forfeited penalty payments for an amount of € 40,000.<sup>6</sup>

37. Pursuant to Article 5:33 of the Awb, a forfeited penalty is paid within six weeks after it has been forfeited by operation of law. The AP has not yet received payment on the date of this decision.

38. It is settled case law of the Administrative Jurisdiction Division of the Council of State that the importance of collecting



forfeited penalty payments must be given a heavy weight. Otherwise, the authority based on the imposition of an order subject to a penalty would be called into question. Collection may be waived in whole or in part only in special circumstances. The AP has not revealed any special circumstances.<sup>7</sup>

6 The AP has here divided the maximum amount of forfeited penalty payments of € 200,000 by five (the five parts of the order).

7 ABRS October 3, 2012, ECLI:NL:RVS:2012:BX8985

7/8

AUTHORITY

PERSONAL DATA

Date Our reference

12 rras ±2:}'3 z2j'>7-KV'5“

5. Decision

39. In view of the above and Article 5:37 Awb, the AP will proceed to collect the penalty of € 40,000 (in words: forty thousand euros) forfeited by the NP, plus the statutory interest.

40. The AP will hand over the aforementioned claim to the Central Judicial Collection Agency (CJIB). After sending this collection order, the NP receives a demand from the CJIB - on behalf of the AP - to pay within two weeks. In the absence of timely payment, the outstanding amount will be increased by the reminder and any collection costs.

Yours faithfully,

If you do not agree with this decision, you can submit a notice of objection pursuant to the General Administrative Law Act, within six weeks after the date on which the decision was sent, to the Dutch Data Protection Authority, PO Box 93374, 2309 AJ The Hague, stating “Awb objection ” on the envelope. Submitting a notice of objection does not suspend the effect of this decision. If urgent urgency, in view of the interests involved, requires it, you can also submit a request for provisional relief to the preliminary relief judge of the district court (administrative law sector ) in the district in which you are domiciled, in which case you must enclose a copy of this decision.

8/8