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.' Hsüg

Date Our reference Your letter from

Subject

Collection 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 grace period included in the penalty decision ran until August 6, 2018. After the grace period had expired, the NP sent documents in which the NP indicated what measures it had taken in response to the imposed 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 periodic penalty payments 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).

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 periodic penalty payments on the NP by means of a penalty decision dated 6 February 2017.1

On August 30, 2017, the NP contacted the AP by telephone with the request to e-mail the contact details (email address and telephone number) of the employee of the AP handling the case 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 to the NP by email dated 30 August 2017.

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

4. By e-mail dated 13 November 2017, the NP informed the AP that a written response regarding compliance with the order subject to periodic penalty payments has fallen out of order 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 29 November 2017, the AP informed the NP that, based on the documents sent on 24 November 2017, it is not sufficiently clear that the order has been (fully) complied with. In this context, the AP has given the NP the opportunity to send additional evidence.

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 that the NP had taken with regard to data processing in N.SIS II.

8. By e-mail dated 6 December 2017, the AP requested further documents to be sent showing that the NP - within the six-month grace period - has complied with the obligation to proactively check the N.SIS II log files for indications of unauthorized access or use of police data.

9. By email dated December 6, 2017, also sent by letter dated December 7, 2017, the NP sent further information to the DPA regarding the proactive monitoring of the N.SIS II log files.

10. In emails dated 31 January, 1, 5 and 6 February 2017, the NP sent further information showing that authorizations before 7 August 2017 are logged by the NP.

1 The findings of the official investigation have been laid down in the final findings report dated 22 October 2015 (hereinafter: the investigation report).

2. The cease and desist order

11. By decision of 6 February 2017, the AP imposed an order subject to periodic penalty payments 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 lead to:

the NP establishes a procedure relating to authorizations for the functional managers of the parties connected to NSIS 11 and the IND employees who process personal data in the context of NSIS II; establish NP personnel profiles that describe the duties 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 connected 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.

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

3. Assessment of compliance with the order subject to periodic penalty payments

14. The AP establishes 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 penalty

order nor the duration of the grace period are under discussion. It is subject to assessment 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 February 6, 2017, it must be concluded that the last day of the grace period was August 6, 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 the NP must take measures in the context of data processing in N.SIS II that lead to a procedure being established that relates to authorizations for the information managers of the network connected to N.SIS II. parties and IND employees who process personal data in the context of N.SIS II.2

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

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

including the procedures and frameworks used to authorize chain partners (including business information managers) and how supervision is organized. The policy document stipulates that the policy will take effect immediately (on 2 August 2017).

18. In view of the foregoing, the AP finds that the NP has complied with part I of the order in time with the adoption of this policy on August 2, 2017.

3.2 With regard to part II of the burden:

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

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

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

3.3 With regard to part III of the burden:

22. The penalty decision stipulates that the NP must take measures in the context of data processing in N.SIS II that lead to periodic checks being carried out on the authorizations granted to the business information managers of the information stored in 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 Chain Partners of August 2, 2017, in which an annual check on authorizations is prescribed. In this context, it has been 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

(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 notes that the NPN has taken measures within the granting period that will result in a periodic (annual) check being carried out on the authorizations granted to the business information managers of the parties connected to N.S1S 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 foregoing, the AP determines that the NP has complied with part III of the order in time.

co

3.4 With regard to part IV of the burden:

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

27. In a letter dated 4 December 2017, the NP reported that changed authorizations are being logged in the generic LAM tool - to which N.SIS II is connected for its authorizations. Furthermore, the NP explained that since October 1, 2016, the IAM tooling offers the possibility to actively monitor and supervise the use of applications. To explain this, the NP has referred to the attached document Implementation Authorization Model Police of 26 September 2016 and the also attached document the Process Description LAM monitoring & control of 9 January 2017. The NP has explained that various functions are used for the logging of N.SIS II authorizations. are configured. In this context, reference was made to the function of keeping a time-trace of the authorization someone has received via IAM. To illustrate this, the NP has included a configuration file from which it can be deduced which details of the authorization process are kept in the history log. In addition, an example report of the authorization history per employee was sent as an attachment to an e-mail dated 5 December 2017, which provides an overview of all authorization changes that have been made for an employee.

28. In e-mails dated 31 January, 1.5 and 6 February 2017, the NP sent further information showing that amended authorizations were already logged by the NP in 2016 and will also be logged after 6 August 2017. The AP notes that the AP has not previously been informed by the NP that changed authorizations were already logged in 2016, even though this should have been the NP's way.3

29. In view of the foregoing, the AP concludes that the NP had already taken measures as referred to in part IV of the order before the penalty decision 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 of the investigation report, which states that the NP does not log changed authorizations (see penalty decision under marginal number 42). The NP has also not objected to the penalty decision, in which this conclusion was reached.

3.5 Part V of the load:

30. The penalty decision stipulates that the NP must take measures in the context of data processing in N.SIS II that lead to regular proactive checks of the log files for indications of unauthorized access or use of police data.

31. In a letter dated 4 December 2017, the NP informed that N.SIS II is connected to the management reporting tool Cognos, with which the responsible managers can check the log files for irregularities. It has also 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 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 has explained that, in the context of data processing in N.SIS II, the log files are not (yet) proactively checked for indications of unlawful access or use of police data. In this context, the NP states that this proactive monitoring is only possible if the Central Works Council (COR) has agreed to this.

33. Whatever else may be about this position of the NP, it does not change the conclusion that part V of the order is not being complied with. For the sake of completeness, the AP 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 grace 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 periodic penalty payment

35. The penalty decision stipulates that if the NPN has not implemented the measures no later than six months after the date of the present penalty decision, the NPN will forfeit a penalty of € 12,500 for each week that the order has not been (fully) implemented until a maximum of € 200,000.

36. In view of the fact that the commencement period ran up to and including August 6, 2017, the AP establishes that penalty payments were forfeited by operation of law on August 14, 20174 5 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 period, account has been taken of the expectation of the NP that the proactive monitoring of the logging could be started in July 2017 (see the recorded report of the conversation between the AP and 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 12 December 2012 ECLI:NL:RVS:2012:BY5884 and ABRS 6 November 2013, ECLI:NL:RVS:2013:1829.

November 26, 2017. Now that the AP has not complied with only one of the five parts of the order, the AP has decided to proceed to collect the forfeited penalty payments in the amount of € 40,000.6

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

38. It is settled case law of the Administrative Jurisdiction Division of the Council of State that a heavy weight must be attached

to the importance of recovering forfeited penalty payments. Otherwise, the authority based on the imposition of an order subject to periodic penalty payments would be undermined. Collection can only be waived in whole or in part in special circumstances. The AP has not revealed any special circumstances.7

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

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

5. Decision

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

40. The AP will hand over the aforementioned claim to the Central Judicial Collection Agency (CJIB). After sending the present collection decision, the NP will receive a reminder 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 an objection under the General Administrative Law Act to the Dutch Data Protection Authority, PO Box 93374, 2309 Aj The Hague, stating “Awb objection” within six weeks of the date of dispatch of the decision. " on the envelope. Submitting a notice of objection does not suspend the operation of this decision. If urgency so requires, in view of the interests involved, you can also submit a request for provisional relief to the provisional relief judge of the court (administrative law sector) in the district in which you live, in which case you must enclose a copy of this decision.