Registered

National Police

attn. the chief of police

[CONFIDENTIAL]

New Explanation 1

2514 BP THE HAGUE

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

Our reference

z2015-00910

Contact

[CONFIDENTIAL]

Your feature

[CONFIDENTIAL]

Date

February 6, 2017

Topic

Charge under penalty

Summary

1. Pursuant to Article 35, second paragraph of the Police Data Act, the Dutch Data Protection Authority (AP) has

(Wpg) viewed in conjunction with Article 60 of the Personal Data Protection Act (Wbp) and Article

44 of 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) and Article 60 of Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the Schengen Information System of the second generation (SIS II) (hereinafter: the Decree) carries out an ex officio investigation into the use of the second generation national Schengen Information System (N.SIS II) by the National Police (hereinafter: the POI). As a result of this investigation, the AP has decided on the basis of Article 35, second paragraph of the Wpg, viewed in conjunction with article 65 of the Wbp and article 5:32, first paragraph, of the General Administrative Law Act (Awb) to impose an order subject to a penalty. With the burden under penalty (hereinafter: the penalty decision) the AP aims to put an end to the detected violations.

2. The penalty decision is intended to take a number of measures. Within the beneficiary period of six months, the charge must be met. In case of non-compliance with the order, the NP is a penalty payment owed of € 12,500 (in words: twelve thousand five hundred euros) for each week that the charge is not (fully) executed up to a maximum of € 200,000 (in words: two hundred thousand euros).

3. The AP bases the penalty decision on the final findings report of 22 October 2015 (hereinafter: research report) and the information subsequently provided by the NP.

Background and course of the procedure

Annex(es) 2

Date

February 6, 2017

Our reference

z2015-00910

4. The investigation report was adopted by the AP on 22 October 2015 and sent to the chief of police. The The public version of the investigation report was published on the AP's website on November 30, 2015.

5. In response to the investigation report, the Minister of Security and Justice has informed the House of Representatives informed by letter dated 7 December 2015 that the NPN will take measures to to end violations found.

6. By letter dated 12 February 2016, the AP informed the NP of its intention to enforce
and the NPN has been given the opportunity to express its views on this intention
to make.

7. On February 18, 2016, the NP adopted the Improvement Plan for the Police Data and Information Security Act, draft version 0.4 of February 2016, submitted to the AP. The final Improvement Plan for the Police Data Act and Information security, from March 2016 (hereinafter: the improvement plan) was submitted to the AP on 9 May 2016. This improvement plan contains an overview of the measures that the NP will take in the coming years to improve comply with the Wpg and also contains the information security measures that must be
lead to the resolution of the deficiencies identified in the Visa investigations
Information System (VIS) and N.SIS II. It is stated in the improvement plan that with the implementation of these measures taken by the police at the end of 2019 (the duration of the programme) largely but not yet completely the Wpg will comply.

8. On March 23, 2016, the NP gave an oral opinion on the
intention to take enforcement action. A report has been made of the hearing. This report is by letter
of 11 May 2016, sent in draft to the NP to give the NP the opportunity to
report to respond.

9. By e-mail dated 24 March 2016, the AP requested the NP to provide in writing and concretely on the basis of substantiate documents which measures the NP has taken or intends to take and
within what period the relevant measures will be implemented.

10. By letter dated April 6, 2016, received on April 11, 2016, the NP responded to this request by providing further provide information.

11. By letter dated 13 May 2016, received on 17 May 2016, the NP responded to the draft report of the hearing. The report of the hearing was adopted by the AP on May 18, 2016. This report and the response of the NP are attached to this penalty decision.

12. By letter dated 13 July 2016, the AP informed the NP that the AP had issued a . in mid-September 2016.
will take a decision with regard to the current enforcement process.

Date

February 6, 2017

Our reference

z2015-00910

13. In a letter dated 1 September 2016, the NP has, in summary, informed the AP that the NP will place the order to perform a security analysis of the process of 'signals' within the NP. The security analysis will begin in September 2016. This analysis is expected to be completed within four months can be completed. In this regard, the NP has requested the decision-making regarding to suspend the enforcement process.

14. In a letter dated September 5, 2016, the AP informed the NP that it sees no reason to take the decision to suspend.

15. In a letter dated 13 September 2016, the NP informed the AP that it has been working on the earlier to implement commitments that are part of the improvement program. In the attachment to this letter, the NP has provided an explanation of the approach to these violations, the state of affairs and the follow-up planning. In addition, the NP has the AP requested to be given the opportunity to explain the measures to be taken by the NP and has again requested the NP to take the decision on any suspend enforcement.

16. Following the latter letter, the AP invited the NP for a meeting on October 4 2016. For the purpose of this conversation, a number of questions were sent to the NP . by e-mail dated September 29, 2016. submitted.

17. By e-mail dated 3 October 2016, the NP replied to the latter e-mail and the NP has sent documents relating to the procedure with regard to the policy with regard to information security incidents.

18. The conversation between the AP and the NP took place on October 4, 2016. During this conversation, the

NP gave an oral explanation of the measures taken and still to be taken by the NP. Of this
conversation, a report was drawn up.

19. By email dated October 7, 2016, the NP sent another document regarding the policy
regarding information security incidents.

20. By letter dated 10 October 2016, sent by e-mail of the same date, the NP – as promised
during the conversation on October 4, 2016 – the AP gave a written explanation about the context
within which the developments in the field of security and the renewal of the
information provision to the NP.

21. On December 5, 2016, at the request of the NP, the AP gave the NP the opportunity to submit a
provide verbal explanations of the context in which the NP operates. During this conversation,
agreed that at the beginning of January 2017 the NP will provide insight into the damage it has affected on the basis of
documents
and measures still to be taken to eliminate the violations found and to provide insight into
the state of affairs in this regard.

22. On January 9, 2017, the NP received a number of documents as a result of the conversation on December 5, 2016
submitted, accompanied by an oral explanation. In summary, the documents relate
on the 2015 incident report, the authorization process, the information security architect and the
progress report on the Q3 2016 improvement plan. The NP also explained that, although the status
of business is that the NP is a bit behind schedule, the expectation is that the final planning is as is
indicated in the appendix to the letter of 13 September 2016, can be realised.

23. By e-mail of January 31, 2017, the POI has submitted the security plan 2017-2019, version 1.0, status final.

sent to the AP. This security plan relates, among other things, to the processing of

police data in the context of N.SIS II.

Research report

24. The reason for this order subject to penalty are the findings in the investigation report of 22

October 2015. The AP concluded in the investigation report that the NP is acting in violation of the

Wpg, the Regulation and the Decree regarding the security and training regulations pertaining to

N.SIS II.

25. With regard to the security regulations, the AP concluded that the NPN in the context of the

data processing in N.SIS II:

a. has not established a security plan;

b. has not properly arranged the access rights and has not set up profiles;

c. has not established a specific written procedure with regard to the authorizations for the

functional managers of the parties affiliated to N.SIS II and the employees of the IND.

Nor does the POI carry out (ongoing) checks on the authorizations granted and there are no

agreements made with the regional units on accountability;

d. does not have a rapid effective and orderly response to an N.SIS II information security incident

laid down in a procedure.

e. does not perform (continuous) checks on the log files and does not log all applications.

26. With regard to the training regulations, the AP concluded that the staff of the NP did not

receive specific and sound training on data security rules and

-protection of N.SIS II and the relevant criminal offenses and sanctions. Furthermore, it has been concluded that

Nor is attention paid to N.SIS II in the general training.

Legal framework

27. The relevant legal framework is formed in particular by the Wpg, the Regulation and the Decree. This

framework is included in Appendix I of this penalty order.

Our reference

z2015-00910

Date

February 6, 2017

Viewpoint NP

28. Following the intention of the AP to take enforcement action, the NP has during the
oral hearing on 23 March 2016. In summary, this view
signifies that it endorses the conclusions established in the investigation report. The NP has in its
pointed out that it attaches importance to the proper security of information and the associated
coherent safeguards for privacy. In order to end the detected violations,
the NP announced to take measures.

Rating

29. The AP establishes that the NP has access rights to N.SIS II and processes police data in that context. This
means, in view of the provisions of Article 2(1) of the Wpg, that the Wpg applies. Furthermore
the Decree and the Regulation apply to data processing. The Regulation and the
Decree contain common provisions on the architecture, financing and
responsibilities, as well as general data processing and data protection rules for SIS II.
In addition to these common rules, the Decree contains specific provisions on processing
of SIS II data for the purpose of judicial and police cooperation in criminal matters, while the
Regulation contains rules for the processing of SIS II data for the implementation of the
policy on the free movement of persons which is part of the Schengen acquis.

30. Pursuant to Article 4, paragraph 3, of the Wpg, the NP must provide appropriate technical and organizational
take measures to protect police data against accidental or unlawful destruction,
against modification, unauthorized communication or access, in particular if the processing is sending
includes data over a network or making available through direct automated access, and against any
other forms of unlawful processing, taking into account in particular the

risks of the processing and the nature of the data to be protected. These measures must, taking into account
taking into account the state of the art and the costs of implementation, an appropriate
guarantee a level of security, taking into account the risks of the processing and the nature of the police data.

31. The AP concludes for the assessment whether there is appropriate technical and organizational
security measures in the further details given in the Code for
Information security, the NEN-ISO/IEC 27002:2013 standard (hereinafter the NEN standard). The NEN standard is a
standard in which internationally applicable measures for information security are elaborated in more detail. if
an organization meets the NEN standard, the AP assumes that Article 4, third, is also met
member of the Wpg.1 In addition, where there is a special regulation for the police, the AP also joins
to the Police Information Security Regulations (Rip). The Rip is a ministerial regulation based on Article
23, first paragraph, under b, of the Police Act 2012. Pursuant to Article 2, first paragraph, of the Rip, this regulation is
applicable to the entire process of information provision and the entire life cycle of
information systems, regardless of the technology used and regardless of the nature of the information.

1 Dutch DPA Guidelines for the Security of Personal Data, February 2013, p. 2

With regard to the security plan

32. Pursuant to Article 4, third paragraph, of the Wpg, the NP must – in summary – provide appropriate technical and
take organizational measures to protect police data against unintentional or
unlawful destruction, against alteration, unauthorized disclosure or access. This means considering
Article 4, opening words and under e, of the Rip, among other things, that the NP must establish an (information) security plan
relating to N.SIS II. This security plan must be explicitly included
what measures the NPN takes to secure the processed data.2 The need to

security plan also follows from Article 10, first paragraph, preamble, of the Decree and Article 10, first paragraph, preamble, of the Regulation.3

33. During the investigation, the NP submitted documents to the AP relating to the security measures within the NP. On the basis of these documents, the AP concluded that these documents cannot be classified as a security plan related to N.SIS II. During the day the hearing of March 23, 2016, the NP, also confirmed by letter of May 13, 2016, to the AP informed that it does not contest the conclusions of the investigation report. In addition, the NP explained that it has several documents relating to the security plan, but that it remains to be assessed which documents need to be revised and indexed could be. In order to put an end to the detected violations, the NP in the improvement plan and to take measures announced in the appendix to the letter of 13 September 2016.4 At e-mail of January 31, 2017, the NP has submitted the security plan 2017-2019, version 1.0, status final AP sent. This security plan relates, among other things, to the processing of police data under N.SIS II. With the transmission of this security plan, the AP establishes that at this point, complied with Article 4, third paragraph, of the Wpg, in conjunction with Article 4, opening words and under e, of the rip.

With regard to access rights to N.SIS II and personnel profiles

34. Pursuant to Article 4, third paragraph, of the Wpg, the NP must – in summary – provide appropriate technical and take organizational measures to protect police data against unintentional or unlawful destruction, against alteration, unauthorized disclosure or access. Access security this is elaborated by means of authorizations and is further specified in Article 6 of the Wpg. The NP must maintain a system of authorizations pursuant to Article 6(1) of the Wpg that meets the requirements of due care and proportionality. The requirements of due care and proportionality is the starting point of the authorization system. These requirements include It is more important that persons are not authorized more widely than necessary for the performance of their duties. 5 This means that the authorizations must be linked to a certain function or functionality.

To this end, the NP must draw up profiles in which the tasks and responsibilities are defined

of persons authorized to access and process personal data in N.SIS II.

2 See also NEN-ISO-IEC 27002:2013, paragraph 5.1.1 and CBP Guidelines for the Security of Personal Data, February 2013,

p. 22

3 It should be noted that Article 10, first paragraph, preamble, of the Decree refers to a security plan, while Article 10,

first paragraph, preamble to the Regulation refers to a safety plan. The same is meant by these terms.

4 However, with regard to all the measures announced by the NPN, it should be noted that they are insufficiently specific

in order to be able to give an opinion with regard to the question of whether these measures will eliminate the violations found.

5 House of Representatives, session year 2005–2006, 30 327, no. 3, p. 34

Date

February 6, 2017

Our reference

z2015-00910

The preparation of personnel profiles serves, among other things, as a means to assess whether the

authorizations are properly arranged. This also follows from the NEN standard6, article 10, first paragraph, under f and g, of

the

Regulation and Article 10, first paragraph, under f and g, of the Decree.

35. The AP has established in the investigation report that the NP is an organization with access rights to N.SIS

II and that it is the administrator of the parties affiliated to N.SIS II. In the research report,

concluded that the NPN has not properly regulated the access rights. In this regard, it has been established that not

all parties that have access rights to N.SIS II are listed in the authorization matrix and that

matrix mentioned parties not all types of access rights are listed. Furthermore, it has been concluded

that the NPN has not drawn up profiles describing the tasks and responsibilities

of persons authorized to view and process personal data in N.SIS II. During the

hearing on March 23, 2016, also confirmed by letter of May 13, 2016, informed the NP that it

does not dispute the conclusions of the investigation report. By letter dated 13 September 2016, the NP issued a appendix containing measures that the NPN intends to take in order to to terminate any violations found. These measures have an implementation period which will run until January 2017. On 9 January 2017, the NP provided an oral explanation in this regard that the NP is lagging behind on this schedule and that this cannot be realized in January 2017, but in June 2017 become. In view of this, the AP concludes that the NP is currently still acting in violation of Article 6, first paragraph, in viewed in conjunction with Article 4(3) of the Wpg.

With regard to the granting of authorizations and the control thereof

36. Pursuant to Article 4(3) of the Wpg, the NP must – in summary – provide appropriate technical and take organizational measures to protect police data against unintentional or unlawful destruction, against alteration, unauthorized disclosure or access. Access security this is elaborated by means of authorizations and is further specified in Article 6 of the Wpg. The NP must maintain a system of authorizations pursuant to Article 6(1) of the Wpg that meets the requirements of due care and proportionality. Pursuant to Article 6, second paragraph, of the Wpg, police data are only processed by officers of the police who are authorized to do so by the responsible are authorized and to the extent that the authorization lasts. To control the To make access security possible, the protocol obligation has been laid down in Article 32 of the Wpg. Article 32, first subsection (c) of the Wpg stipulates that the responsible party is responsible for the written recording of the granting of the authorizations, as referred to in Article 6 of the Wpg.

These legal provisions have been further elaborated in the NEN standard, whereby for the purpose of management of access rights requires that a formal registration and deregistration procedure must be implemented to enable allocation of access rights.7 In addition, the access rights of users should be regularly assessed.8 This also follows from article 10, first paragraph, under f and k, of the Regulation and Article 10, first paragraph, under f and k, of the Decree.

6 NEN-ISO-IEC 27002:2013, paragraph 9.1.1 and paragraph 9.2.1.

7 NEN-ISO-IEC 27002:2013, paragraph 9.2.1. See also Dutch DPA Guidelines for the Security of Personal Data, February

2013, p. 22

8 NEN-ISO-IEC 27002:2013, paragraph 9.2.5

Date

February 6, 2017

Our reference

z2015-00910

37. The AP concluded in the investigation report that the (National Unit of the) NP does not have a formal established procedure that relates to the authorizations for the functional managers of the Parties affiliated to N.SIS II and IND employees who work in the context of N.SIS II process personal data. In addition, it has been concluded in this context that the NP is not a (periodic) carries out checks on the parties affiliated to N.SIS II and the affiliated parties to the functional managers authorizations granted to employees of the IND in the context of N.SIS II.

38. At the hearing of March 23, 2016, also confirmed by letter of May 13, 2016, the NP informed the AP informed that it does not contest the conclusions of the investigation report. By the letter of September 13 In 2016, the NPN added an appendix containing measures that the NPN intends to take to put an end to the violations found. These measures have a implementation period that runs up to and including January 2017. On January 9, 2017, the NP has Orally explained that the NP is lagging behind on this schedule and that this is not in January 2017, but in June 2017 can be realized. In view of this, the AP determines with regard to the granting of authorizations that the NPN does not yet have a formally established procedure related to authorizations for the functional managers of the parties affiliated to N.SIS II and the employees of the IND who work in the process personal data under N.SIS II. As a result, the NP is still acting in conflict with Article 6, first paragraph, in conjunction with Article 4, third paragraph, of the Wpg, the NEN standard9, Article 10, first paragraph, under f, of the Regulation and Article 10, first paragraph, under f, of the Decree. With regard to the

(ongoing) check on granted authorizations, the NP establishes that the NP does not have a (periodic) check performs on the to the functional managers of the parties affiliated to N.SIS II and to the authorizations granted to employees of the IND. The NP is also still trading in this contrary to article 6, first paragraph, viewed in conjunction with article 4, third paragraph, of the Wpg and article 32, first member, under c, of the Wpg.

Regarding the security incidents

39. Pursuant to Article 4, third paragraph, of the Wpg, the NP must – in summary – provide appropriate technical and take organizational measures to protect police data against unintentional or unlawful destruction, against alteration, unauthorized disclosure or access. This means considering Article 3, second paragraph, under f, of the Rip, among other things, that the NP must adopt a policy document which lays down the manner in which established or suspected infringements of the information security are reported by police officers, the police officer to whom these breaches are reported and the manner in which they are handled. The NEN standard specifies this in more detail, namely that there should be a consistent and effective approach to the management of information security incidents, including communications about security events and security vulnerabilities. To this end, management responsibilities and procedures should be be established to ensure a rapid, effective and orderly response to information security incidents

10 This also follows from Article 10, first paragraph, under d, of the Regulation and Article 10, first paragraph paragraph, under d, of the Decree.

9 NEN-ISO-IEC 27002:2013, paragraph 9.1.1. and section 9.2.1. See also Dutch DPA Guidelines for the Security of Personal Data, February 2013, p. 22

10 NEN-ISO-IEC 27002:2013, paragraph 16.1.1

Date

February 6, 2017

40. In the investigation report, the AP concluded that the NP has not established a procedure against
regarding the management of information security incidents under N.SIS II and that therefore
there is no rapid, effective and orderly response to information security incidents.
At the hearing of March 23, 2016, also confirmed by letter of May 13, 2016, the NP informed the AP
informed that it does not contest the conclusions of the investigation report. In order to determine the
to have violations terminated, the NP has stated in the appendix to the improvement plan and in the appendix to the letter
announced to take measures on 13 September 2016. By e-mail dated October 3, 2016, the NP
sent documents relating to the procedure with regard to the policy with regard to
information security incidents. This policy was explained verbally during a conversation with the AP on 4
October 2016. By e-mail dated October 7, 2016, the NP sent another document related to
has on the policy regarding information security incidents. With the sending of this
documents and the explanation given during the meeting of 4 October 2016, in which it was stated that the
established procedure regarding information security incident policy
also relates to the processing of data in the context of N.SIS II, the AP notes that on this
Article 4(3) of the Wpg is complied with in conjunction with Article 3(2),
under f, of the Rip.
With regard to logging and (continuous) checks on the use of N.SIS II
41. Pursuant to Article 4(3) of the Wpg, the NP must – in summary – provide appropriate technical and
take organizational measures to protect police data against unintentional or
unlawful destruction, against alteration, unauthorized disclosure or access. This means, in view of
the interpretation given by the NEN standard11, that log files of events that
record user activities, exceptions and information security events should be
be made, stored and regularly reviewed.12 This also follows from Article 10(1),
under i and k, of the Regulation and Article 10, first paragraph, under i and k, of the Decree.

42. In the investigation report, the AP concluded that the NP does not regularly update the log files checks. It has been established that checking the logging only takes place (in retrospect) if there is of security signals, integrity investigations, complaints or a technical malfunction. The log files are not periodically proactively monitored for indications of unauthorized access or unlawful use of police data. In addition, the AP concluded that changed authorizations in N.SIS II are not logged by the POI. At the hearing on March 23, 2016, also confirmed by letter dated 13 In May 2016, the NP informed the AP that it does not dispute the conclusions of the investigation report. In order to put an end to the violations found, the NP has in the annex to the letter dated 13 announced to take measures in September 2016, stating an implementation period that runs until April 2017. During the meeting on October 4, 2016, the NP explained that the control of log files cannot yet proactively take place at the POI, because the act is subject to consent on pursuant to the Works Councils Act, and the Works Council has not yet agreed to this.

11 NEN-ISO-IEC 27002:2013, paragraph 12.4.1.

12 See also Dutch DPA Guidelines for the Security of Personal Data, February 2013, p. 22

43. In view of the foregoing, the AP finds that the NP, due to the lack of a regular proactive monitoring of the log files and due to the fact that changed or deleted authorizations in N.SIS II are not logged by the NP, currently still acts in violation of Article 4(3) of the wpg.

With regard to the training regulations

44. Pursuant to Article 4, third paragraph, of the Wpg, the NP must – in summary – provide appropriate technical and take organizational measures to protect police data against unintentional or

unlawful destruction, against alteration, unauthorized disclosure or access. Information security encompasses all measures by which organizations protect their information. Offering a appropriate training can be regarded as an organizational measure and, in view of the interpretation given by the NEN standard13, that all employees of the organization and, insofar as relevant, contractors provide appropriate awareness education and training and regular upskilling of policies and procedures of the organization, as relevant to their position.14

The provision of appropriate training also follows from Article 14 of the Regulation and Article 14 of the Decision.

45. With regard to the training provided by the NP, the AP concluded in the investigation report that the staff of the NP does not receive specific and sound training with regard to the rules on data security and protection of N.SIS II and the relevant criminal offenses and sanctions and that Nor is attention paid to N.SIS II in the general training.

46. Following this report, the NP, both during the hearing and by letter dated 6 April 2016, issued a further explanation given on the training program of the NP. In this regard, in summary explained that the generic training/courses, which are organized in consultation with the Police Academy developed, do not contain specific N.SIS II aspects, but that where employees have specific have rights to create or delete alerts within N.SIS II, the NP uses a 'train the trainer concept', using the User Manual SMC. In addition it has been explained that during the training, attention is paid to the relevant criminal offenses and sanctions related to the information security policy.

47. In view of what was put forward during the hearing and the documents submitted subsequently, the In this context, the AP has established that there is no longer any question of a violation within the meaning of Article 4, third paragraph, of the Wpg.

Order subject to penalty and beneficiary period

48. The AP decides to impose an order subject to a penalty under Article 35, second paragraph of the

Wpg, viewed in conjunction with Article 65 of the Wbp and Article 5:32(1) of the Awb. this burden

13 NEN-ISO-IEC 27002:2013, section 7.2.2.

14 See also Dutch DPA Guidelines for the Security of Personal Data, February 2013, p. 22

subject to a penalty is aimed at ending the detected violations and preventing

repetition, as referred to in Article 5:2, first paragraph, under b, of the Awb.

49. The AP orders the NP to take measures within the beneficiary period referred to below

in order to remove the unlawful nature of the processing. This means that NP within this

period must ensure that further violation of Article 4, third paragraph, of the Wpg, Article 6, first

paragraph, of the Wpg and Article 32, first paragraph, under c, of the Wpg is omitted.

50. In concrete terms, this means that the NP must have a formally established procedure that relates to

to the authorizations for the functional managers of the parties affiliated to N.SIS II and the

employees of the IND. The AP points out that this must be a formal registration and

opt-out procedure to enable assignment of access rights.15 These procedures serve

all stages in the user access life cycle, user access, from the first registration of

new users until the eventual opt-out of users who no longer have access to

information systems and services.16

51. The NPN must also establish personnel profiles in which the tasks and responsibilities are defined

of persons authorized to access and process personal data in N.SIS II.17

52. Furthermore, the NP must ensure that a periodic check is carried out on the authorizations

assigned to the functional managers of the parties affiliated to N.SIS II and the

employees of the IND.18

53. Furthermore, it is required that the NP logs changed authorizations in N.SIS II.19

54. In addition, in the context of N.SIS II, the NPN should regularly check log files for indications of unauthorized access or use of police data. This means that not only afterwards an audit (in the case of security signals, integrity investigations, complaints or a technical failure) must take place, but that the log files must also be proactively regularly are monitored for indications of unauthorized access or use of police data.20

Beneficiary term

55. Article 5:32a, second paragraph, of the Awb provides that a beneficiary period is set 'during which the violator can carry out the order without forfeiting a penalty." In the Memoir of

15 NEN-ISO-IEC 27002:2013, paragraph 9.2.1.

16 See also Dutch DPA Guidelines for the Security of Personal Data, February 2013, p. 22

17 NEN-ISO-IEC 27002:2013, paragraph 9.1.1 and paragraph 9.2.1.

18 NEN-ISO-IEC 27002:2013, paragraph 9.2.5

19 NEN-ISO-IEC 27002:2013, paragraph 12.4.1. See also Dutch DPA Guidelines for the Security of Personal Data, February 2013, p. 22

20 NEN-ISO-IEC 27002:2013, paragraph 12.4.1. See also Dutch DPA Guidelines for the Security of Personal Data, February 2013, p. 22

Explanation to the General Administrative Law Act, it is emphasized that this period should be as short as possible, but long enough to allow to carry the load.21

56. The AP attaches a grace period of six months to the order subject to a penalty. The AP has
determining the beneficiary period taking into account the context in which the
developments in security and the renewal of information provision at the NPN, such as
was explained by the NP in a letter dated 10 October 2016 and subsequently explained orally on behalf of the NP.
In the opinion of the AP, a period of six months is reasonable with a view to terminating the
detected violations and the prevention of further violations.
57. Article 5:32b, third paragraph, of the Awb prescribes that the penalty amounts are in reasonable proportion
to the gravity of the harmed interest and to the intended effect of the penalty. In the latter case
It is important that a penalty payment must provide such an incentive that the order is complied with.
58. If the NP does not end the violations found within six months, she forfeits a
penalty. The AP sets the amount of this penalty at € 12,500 for every week that the order is not paid
(entirely) executed up to a maximum of € 200,000. In the opinion of the Authority, the
amount of these amounts in reasonable proportion to the gravity of the violation caused by the violation
interest - the protection of police data and the privacy of those involved - and
are they (further) high enough to induce the NP to end the violations.
21 Parliamentary Papers II 1993/94, 23 700, no. 3, p.163.

Date
February 6, 2017
Our reference
z2015-00910
dictum
The AP imposes an order subject to penalty on the NP with the following content:
Within six months of the date of this decision, the NP must within the framework of the data processing
take measures in N.SIS II that result in:
i.

the NP establishes a procedure relating to authorizations for the functional managers

of the parties affiliated to N.SIS II and the employees of the IND who work in the context of N.SIS

II process personal data;

establishes the NP personnel profiles in which the tasks and responsibilities are defined

of persons authorized to access and process personal data in N.SIS II

process;

the NP ensures that a periodic check is carried out on the authorizations that are

allocated to the functional managers of the parties affiliated to N.SIS II and the

employees of the IND;

changed authorizations are logged;

the log files are regularly proactively checked for indications of illegal

access or unlawful use of police data.

II.

III.

IV.

v.

If the NP has not taken the measures no later than six months after the date of this penalty decision

executed, the NP forfeits a penalty of €12,500 (in words: twelve thousand five hundred euros) for

every week that the load has not been (fully) carried out up to a maximum of € 200,000 (in words:

two hundred thousand euros).

Yours faithfully,

Authority Personal Data,

w.g.

mr. A. Wolfsen

Chair

Remedies

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.

13/18

Date

February 6, 2017

Our reference

z2015-00910

Annex 1 – legal framework

Personal Data Protection Act (Wbp)

Article 51, first paragraph, of the Wbp (insofar as relevant):

1. There is a Personal Data Protection Board that has the task of supervising the processing of

personal data in accordance with the provisions laid down by and pursuant to the law. The College also holds

supervision of the processing of personal data in the Netherlands, when the processing takes place

in accordance with the law of another country of the European Union.

[…]

Article 60, first and second paragraph, of the Wbp:

1. The Board may, ex officio or at the request of an interested party, initiate an investigation into the

the manner in which the provisions of or . are applied with regard to data processing

under the law.

2. The College shall notify its provisional findings to the person responsible or the group of

responsible parties involved in the investigation and gives them the opportunity to express their views

to give on it. If the preliminary findings are related to the implementation of any law, then

the Board shall also notify Our Minister concerned.

[…]

Article 61, first and fourth paragraph, of the Wbp (insofar as relevant):

1. The members and extraordinary are charged with the supervision of compliance as referred to in Article 51, first paragraph

members of the College, the officials of the secretariat of the College, as well as the

College designated persons.

[…]

4. The Board is authorized to impose an order under administrative coercion to enforce Article 5:20,

first paragraph, of the General Administrative Law Act, insofar as it concerns the obligation to grant

cooperation with an official designated by or pursuant to the first paragraph.

[…]

Article 65 of the Wbp:

The Board is authorized to impose an order under administrative coercion to enforce the

obligations under this Act.

General Administrative Law Act (Awb)

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

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

impose an order subject to penalty on the offender.

Date

February 6, 2017

Our reference

z2015-00910

Police Data Act (Wpg)

Article 2, first paragraph, Wpg:

1. This law applies to the processing of police data that is included in a file or

intended to be included therein.

Article 4, paragraph 3, of the Wpg:

3. The controller takes appropriate technical and organizational measures to collect police data

secure against accidental or unlawful destruction, alteration, unauthorized disclosure or access, in particular where processing data transmission over a network or making available through 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 6 of the Wpg (insofar as relevant)

1. The responsible person maintains a system of authorizations that meets the requirements of due diligence and proportionality.

2. Police data will only be processed by police officers who have been authorized by the responsible are authorized and to the extent that the authorization lasts.

3. The person in charge authorizes the police officers under his control for the processing of police data to carry out the parts of the police task with which they are involved charge. The authorization contains a clear description of the processing operations to which the relevant party is responsible official is authorized and the parts of the police task for the performance of which the processing is done.

Article 32, first paragraph, of the Wpg (insofar as relevant):

1. The responsible party is responsible for the written recording of:

[…]

c. the granting of the authorizations referred to in Article 6;

[…]

Article 35, first and second paragraph, of the Wpg

1. The Personal Data Protection Board 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.

15/18

Date

February 6, 2017

Our reference

z2015-00910

Police Information Security Regulations (Rip)

Article 2, first paragraph, of the Rip:

1. This regulation applies to the entire process of information provision and the entire

life cycle of information systems, regardless of the technology applied and regardless of the nature of the

information.

Article 3, first and second paragraph, of the Rip (if relevant):

1. The chief of police establishes the information security policy in a policy document and disseminates this policy.

If the information security policy also relates to information systems for the benefit of the

investigation of criminal offences, the chief of police adopts this policy document after consultation with the chief officer

of justice.

2. The document includes at least:

[…]

f. the manner in which established or suspected breaches of information security by

police officers, the police officer to whom these violations are reported and the

way in which these are handled;

[…]

Article 4, preamble and under e, of the Rip:

The chief of police ensures that for each information system and for each common IT

service in a systematic manner taking into account the reliability criteria and standard classes,

referred to in Annex I, it is determined which system of measures under information security

should be affected. This duty of care means at least that:

[…]

e. an information security plan for each information system and for each common IT service

is established. In any case, this includes:

1. an action plan to implement all security measures;

2. a calamity paragraph whose effectiveness is periodically tested.

Police Act 2012

Article 23, first paragraph, under b, of the Police Act 2012

1. Rules may be laid down by ministerial regulation about:

a. […]

b. information security by the police and other organizations as referred to in part a.

16/18

Date

February 6, 2017

Our reference

z2015-00910

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) and Council Decision 2007/533/JHA of 12 June 2007

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

generation (SIS II) (hereinafter: the Decree)

Article 10, first paragraph, of the Decree and the Regulation22 (insofar as relevant):

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

so that:

[…]

d) unauthorized data storage in the memory, as well as unauthorized access, modification or

deletion of stored personal data is prevented (storage control);

[…]

f) those authorized to use an automatic data processing system,

have access only to the data to which their access authorization relates, and

only with personal and unique user identities and secret access procedures (control

on access to the data);

(g) ensure that all authorities with a right of access to SIS II or to facilities for

data processing, drawing up profiles that describe the tasks and responsibilities

of persons authorized to access, enter, update, delete and

search them, and make these profiles available without delay on request to the persons referred to in Article 60

national supervisory authorities referred to (personnel profiles);

[…]

i) it can be subsequently verified and established which personal data, when, by whom and for

which purpose are included in an automated data processing system (checking the

inclusion);

[…]

(k) the effectiveness of the security measures referred to in this paragraph is continuously monitored

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

ensure that the requirements of this Decree are complied with (internal control).

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 in their territory and the transfer from that territory, and the

exchange and further processing of additional information.

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

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

22 It should be noted that the articles of the Decree correspond to those of the Regulation. The only difference is that in Article 10, first paragraph, preamble, of the Decree refers to a security plan, while Article 10, first paragraph, preamble of the Regulation

talks about a security plan. The same is meant by these terms.

Date

February 6, 2017

Our reference

z2015-00910

3. Member States shall ensure that sufficient resources are available to national supervisory authorities

to carry out their duties under this Regulation.

Article 60 of the Decree:

1. Each Member State shall ensure that an independent authority (‘national supervisory authority’) is autonomous

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 carried out in accordance with international auditing standards.

3. Member States shall ensure that sufficient resources are available to the national supervisory authority

to carry out its duties under this Decision.