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

authoritypersonal data.nl

Our reference

z2015-00910

Contact

[CONFIDENTIAL]

Your feature

[CONFIDENTIAL]

Date

February 6, 2017

Subject

Load under duress

Resume

1. Pursuant to Article 35, paragraph 2 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) conducted an ex officio investigation into the use of the second generation National Schengen Information System (N.SIS II) by the National Police (hereinafter: the NP). As a result of this investigation, the AP has decided, pursuant to 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 periodic penalty payments. With the load under duress (hereinafter: the penalty decision) the DPA aims to put an end to the established violations.

2. The penalty decision serves to take a number of measures. Within the beneficiary period of six months, the burden must be met. In case of non-compliance with the order, the NP is a penalty owed € 12,500 (in words: twelve thousand five hundred euros) for each week that the burden is not has been carried out (in full) 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

1

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 public version of the research report was published on November 30, 2015 on the website of the AP.

5. Following the investigation report, the Minister of Security and Justice has asked the House of Representatives informed by letter dated 7 December 2015 that the NP will take measures to reduce the to terminate identified violations.

6. In a letter dated 12 February 2016, the AP informed the NP of its intention to take enforcement action on
and the NP has been given the opportunity to express its views on this intention
to make.

7. On 18 February 2016, the NP approved 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, dated March 2016 (hereinafter: the improvement plan) was submitted to the AP on 9 May 2016. This improvement plan contains an overview of the measures to be taken by the NP in the coming years to comply with the Wpg and also contains the information security measures that must be taken lead to the resolution of the shortcomings identified in the Visa investigations Information System (VIS) and N.SIS II. It is stated in the improvement plan that with the implementation of this At the end of 2019 (the duration of the programme), the police will largely, but not yet fully, implement the Wpg will comply.

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

9. In an e-mail dated 24 March 2016, the AP requested the NP to provide written and concrete information based on substantiate in writing which measures the NP has taken or intends to take and within which 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 The NP's response are attached to this penalty decision.

12. In a letter dated 13 July 2016, the AP informed the NP that in mid-September 2016 the AP will make a decision with regard to the present enforcement procedure.

Date

February 6, 2017

Our reference

z2015-00910

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

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

15. In a letter dated 13 September 2016, the NP informed the AP that since the beginning of 2016 it has been working on the earlier commitments that are part of the improvement program. In the attachment to this letter, the NP has provided an explanation of the violations found approach to these violations, the current situation and the follow-up planning. In addition, the NP has the AP requested to be given the opportunity to provide an explanation during an interview measures to be taken by the NP and has again requested the NP to decide on any suspend enforcement.

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

17. By e-mail of 3 October 2016, the NP responded to the latter e-mail and the NP documents pertaining 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 was given 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 of October 7, 2016, the NP sent another document regarding the policy regarding information security incidents.

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

21. On December 5, 2016, at the request of the NP, the AP gave the NP the opportunity to to provide an oral explanation of the context in which the ANP operates. During this conversation agreed that at the beginning of January 2017 the NP will provide information on the basis of documents that it has affected and measures still to be taken to remove the observed violations and to provide insight into the state of affairs in this regard.

22. On 9 January 2017, following the meeting of 5 December 2016, the NP submitted a number of documents submitted, accompanied by an oral explanation. In summary, the documents are relevant 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 the fact is that the NP is somewhat behind schedule, the expectation is that the final planning is as it is indicated in the appendix to the letter of 13 September 2016, can be realized.

23. By email dated January 31, 2017, the NP submitted the security plan 2017-2019, version 1.0, status final to

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 periodic penalty payments is the findings in the investigation report of 22 October 2015. The AP has concluded in the investigation report that the NP is acting contrary to the Wpg, the Regulation and the Decree regarding the security and training regulations that pertain to N.SIS II.

25. With regard to the security regulations, the AP has concluded that the ANP in the context of the data processing in N.SIS II:

a. has not established a security plan;

b. has not properly arranged access rights and has not created profiles;

c. has not established a specific written procedure regarding the authorizations for the functional managers of the parties connected to N.SIS II and the employees of the IND. Nor does the NP carry out (ongoing) checks on the granted authorizations and there are none made agreements with the regional units about 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 (ongoing) checks on the log files and does not log all applications.

26. With regard to the training regulations, the AP has concluded that the NP's personnel have no receive specific and sound training with regard to data security rules and -protection of N.SIS II and the relevant offenses and sanctions. It has also been concluded that neither is attention paid to N.SIS II in the general training.

Legal framework

27. The relevant legal framework is mainly formed by the Wpg, the Regulation and the Decree. This framework is included in Annex I to this penalty decision.

Our reference

z2015-00910

Date

February 6, 2017

View NP

28. In response to the AP's intention to take enforcement action, the NP during the
oral hearing of 23 March 2016. In summary, this is the point
that it endorses the conclusions drawn in the investigation report. The NP has in her
point out that it attaches importance to proper information security and the associated security
related safeguards for privacy. In order to end the observed violations
the NP announced that it would take measures.

Judgement

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 on data processing apply. The Regulation and the
Decision contain common provisions on the architecture, financing and the
responsibilities, as well as general data processing and protection rules for SIS II.
Apart from these common rules, the Decree contains specific provisions on processing
of SIS II data for judicial and police cooperation in criminal matters, while the
Regulation contains rules for the processing of SIS II data for the purpose of implementing it
policy on the free movement of persons which is part of the Schengen acquis.

30. Pursuant to Article 4(3) of the Wpg, the NP must provide appropriate technical and organizational
take measures to protect police data against accidental or unlawful destruction,
against alteration, unauthorized communication or access, in particular if the processing involves transmission of
includes data 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 to be protected. These measures must be taken into account
taking into account the state of the art and the costs of implementation, an appropriate
guarantee a level of security, given the risks of the processing and the nature of the police data.
31. The AP closes before assessing whether there are appropriate technical and organizational requirements
security measures with 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 one
standard in which internationally applicable measures for information security are further elaborated. If
an organization complies with the NEN standard, the AP assumes that it also complies with Article 4, third
member of the Wpg.1 In addition, the AP joins in where there is a special arrangement for the police
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
applies 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 CBP Guidelines on the Protection of Personal Data, February 2013, p. 2

Regarding the security plan
32. 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 accidental or
unlawful destruction, against alteration, unauthorized communication or access. This means paying attention
Article 4, preamble and under e, of the RIP, among other things, that the NP must draw up an (information) security plan
that pertains to N.SIS II. This security plan must explicitly include
what measures the NP takes to secure the processed data.2 The need to have a

to adopt a security plan also follows from Article 10, paragraph 1, opening words, of the Decree and Article 10, first paragraph, preamble, of the Regulation.3

33. During the investigation, the NP submitted documents to the AP that relate to the security measures within the NP. Based on these documents, the AP has concluded that these documents cannot be regarded 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 dispute the conclusions of the investigation report. In addition, the NP explained that it has several documents related to the security plan, but that it remains to be assessed which documents should be reviewed and indexed could be. In order to put an end to the observed violations, the NP in the improvement plan and measures announced in the appendix to the letter of 13 September 2016.4 At e-mail dated January 31, 2017, the NP has sent the security plan 2017-2019, version 1.0, status final, to the AP sent. This security plan relates, among other things, to the processing of police data in the context of N.SIS II. With the sending of this security plan, the AP determines that this point is complies with Article 4, third paragraph, of the Wpg, viewed in conjunction with Article 4, preamble and under e, of the Rip.

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

34. 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 accidental or unlawful destruction, against alteration, unauthorized communication or access. Access security This has been 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 diligence and proportionality are the starting point of the authorization system. These requirements include also note that persons are not authorized more widely than necessary for the fulfillment 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 specified

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

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

p. 22

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

The opening paragraph of the Regulation refers to a safety plan. These terms mean the same thing.

4 However, with regard to all measures announced by the NP, it should be noted that they are not sufficiently specific

to be able to give an opinion with regard to the question whether these measures will remedy the observed violations.

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

Date

February 6, 2017

Our reference

z2015-00910

Drawing up personnel profiles serves, among other things, as a means of assessing 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(1)(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 connected to N.SIS II. In the research report

concluded that the NPN did not regulate access rights correctly. It has been established that this is not the case

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

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

that the NP has not drawn up profiles in which the tasks and responsibilities are described

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

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

the conclusions of the investigation report are not contested. In a letter dated 13 September 2016, the NP issued a
appendix containing measures that the NP intends to take in order to achieve the
rectify established violations. These measures have an implementation period
which runs until January 2017. On 9 January 2017, the NP explained this orally
that the NP is lagging behind on this planning 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 accidental or
unlawful destruction, against alteration, unauthorized communication or access. Access security
This has been 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(2) of the
Wpg, police data will only be processed by police officers who have been authorized by the
responsible are authorized and insofar as the authorization extends. To control the
To make access security possible, the protocol obligation is laid down in Article 32 of the Wpg. Article 32, first
paragraph, under c, of the Wpg stipulates that the controller 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 elaborated in more detail in the NEN standard, with the benefit of management
access rights stipulate that a formal registration and logout procedure must be carried out
implemented to enable allocation of access rights.7 Furthermore, the
users' access rights should be reviewed regularly.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, section 9.1.1 and section 9.2.1.

7 NEN-ISO-IEC 27002:2013, section 9.2.1. See also CBP Guidelines on the Protection of Personal Data, February 2013, p. 22

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

Date

February 6, 2017

Our reference

z2015-00910

37. The AP has 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 business information managers of the Parties affiliated to N.SIS II and IND employees who are registered in the context of N.SIS II process personal data. In addition, it has been concluded in this context that the NP does not have (periodic) checks the functional managers of the parties connected to N.SIS II and the to IND employees granted authorizations in the context of N.SIS II.

38. During the hearing of March 23, 2016, also confirmed by letter of May 13, 2016, the NP told the AP informed that it does not dispute the conclusions of the investigation report. By letter of 13 September In 2016, the NP added an appendix containing measures that the NP intends to implement to put an end to the observed violations. These measures have a implementation term that runs up to and including January 2017. On 9 January 2017, the NP explained orally that the NP is behind schedule and that this will not be in January 2017, but in June can be achieved in 2017. In view of this, the AP determines with regard to the granting of authorizations that the NP does not yet have a formally established procedure that relates to authorizations for the functional administrators of the parties connected to N.SIS II and the IND employees who work in the process personal data within the framework of N.SIS II. As a result, the NP is still acting contrary to 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) checks on granted authorizations, the ANP establishes that the ANP does not have a (periodic) check

performs on the functional managers of the parties connected to N.SIS II and on the
employees of the IND granted authorizations. The NP is also still trading in this respect insofar as this
conflict with Article 6, first paragraph, viewed in conjunction with Article 4, third paragraph, of the Wpg and Article 32, first
paragraph, under c, of the Wpg.

Regarding the security incidents

39. 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 accidental or
unlawful destruction, against alteration, unauthorized communication or access. This means paying attention
Article 3(2)(f) of the RIP states, among other things, that the NP must adopt a policy document
which lays down the manner in which detected or suspected infringements of the
information security are reported by police officers, the police officer to whom these breaches occur
are reported and how they are handled. The NEN standard specifies this in more detail, namely
that a consistent and effective approach to the management of
information security incidents, including security event communications and
security vulnerabilities. Management responsibilities and procedures should be for this purpose
be established to ensure a prompt, effective and orderly response to information security incidents
to be achieved.10 This also follows from Article 10(1)(d) of the Regulation and Article 10(1)
paragraph, under d, of the Decree.

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

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

40. In the investigation report, the AP concluded that the NP has not established a procedure against regarding the management of information security incidents in the context of N.SIS II and therefore there is no prompt, effective and orderly response to information security incidents.

During the hearing of March 23, 2016, also confirmed by letter of May 13, 2016, the NP told the AP informed that it does not dispute the conclusions of the investigation report. At the end of the observed the NP has stated in the appendix to the improvement plan and in the appendix to the letter announced on 13 September 2016 to take measures. In an email dated October 3, 2016, the NP documents pertaining 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 of October 7, 2016, the NP sent another document relating to has on the policy regarding information security incidents. With the transmission of this documents and the explanation given during the interview of October 4, 2016, in which it is stated that the established procedure with regard to the policy with regard to information security incidents also relates to the processing of data in the context of N.SIS II, the AP notes that this point, Article 4(3) of the Wpg is complied with, viewed in conjunction with Article 3(2), under f, of the Rip.

With regard to the logging and the (ongoing) 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 accidental or unlawful destruction, against alteration, unauthorized communication or access. This means, considering the interpretation given by the NEN standard11, that log files of events that log user activities, exceptions and information security events be made, stored and regularly assessed.12 This also follows from Article 10, first paragraph, 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 the check on the logging only takes place (afterwards) in the event that there is of safety signals, integrity investigations, complaints or a technical malfunction. The log files are not periodically proactively checked for indications of unauthorized access or unauthorized use use of police data. In addition, the AP has concluded that changed authorizations in N.SIS II not be logged by the POI. At the hearing of 23 March 2016, also confirmed by letter dated 13 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 observed violations, the NP has added in the appendix to the letter of 13 announced in September 2016 that it would take measures, with an implementation term specified runs through April 2017. During the interview on October 4, 2016, the NP explained that the control of log files cannot yet proactively take place at the ANP, because the action is subject to consent under the Works Councils Act, and the works council has not yet agreed to this.

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

12 See also CBP Guidelines on the Protection of Personal Data, February 2013, p. 22

43. In view of the foregoing, the AP notes that the NP due to the lack of a regular proactive control 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 violates Article 4, paragraph 3, of the Wpg.

With regard to the training regulations

44. 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 accidental or unlawful destruction, against alteration, unauthorized communication or access. Information security

comprises the entirety of measures with which organizations secure their information. Providing a appropriate training can be regarded as an organizational measure and, given the interpretation given by the NEN standard13, that all employees of the organization and, insofar as relevant, contractors receive appropriate awareness education and training and regular refresher training organizational policies and procedures, as relevant to their position.14

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

45. With regard to the training offered 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 neither 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 of the training program of the NP. In this regard, summarized explained that the generic training/courses, which are developed in consultation with the Police Academy developed, do not contain specific N.SIS II aspects, but 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 SMC User Manual. In addition it has been explained that during the training courses 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 AP has established in this context that there is currently no longer a violation within the meaning of Article 4, third paragraph, of the Wpg.

Order subject to periodic penalty payments and grace period

48. The AP decides to impose an order subject to periodic penalty payments pursuant to Article 35, paragraph 2 of the Wpg, viewed in conjunction with Article 65 of the Wbp and Article 5:32, first paragraph, of the Awb. This burden

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

14 See also CBP Guidelines on the Protection of Personal Data, February 2013, p. 22

Date

February 6, 2017

Our reference

z2015-00910

subject to periodic penalty payments is aimed at ending the established violations and preventing repetition, as referred to in Section 5:2(1)(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 implies that NP within this term should 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 ANP must have a formally established procedure that relates on the authorizations for the functional managers of the parties connected to N.SIS II and the employees of the IND. The AP points out that this must be a formal registration logout procedure to allow assignment of access rights.15 These procedures serve all stages in the user access lifecycle, user access, from the initial registration of new users to the final logout of users who no longer have access to information systems and services.16

51. The NPN should also establish personnel profiles in which the tasks and responsibilities are specified of persons authorized to view and process personal data in N.SIS II.17

52. Furthermore, the NPN must ensure that a periodic check is carried out on the authorisations assigned to the functional managers of the parties connected to N.SIS II and the employees of the IND.18

53. It is also required that the NP logs changed authorizations in N.SIS II.19

54. In addition, in the context of N.SIS II, the NP should regularly check log files for indications of unauthorized access or use of police data. This means not just afterwards an audit (in the event of safety signals, integrity investigations, complaints or a technical failure) must take place, but that the log files must also be proactive on a regular basis are checked for indications of unauthorized access or use of police data.20

Beneficiary term

55. Article 5:32a, paragraph 2, of the Awb stipulates that a grace period is set 'during which the offender can carry out the order without forfeiting a penalty'. In the Memoir of

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

16 See also CBP Guidelines on the Protection of Personal Data, February 2013, p. 22

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

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

19 NEN-ISO-IEC 27002:2013, section 12.4.1. See also CBP Guidelines on the Protection of Personal Data, February 2013, p. 22

20 NEN-ISO-IEC 27002:2013, section 12.4.1. See also CBP Guidelines on the Protection of Personal Data, February 2013, p. 22

Explanatory notes to the Awb emphasize that this period should be as short as possible, but long enough to to be able to carry out the load.21

56. The DPA attaches a grace period of six months to the order subject to periodic penalty payments. The AP has the determination of the beneficiary period takes into account the context within which the

developments in security and the renewal of information provision at the NP take place, 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 stipulates that the penalty amounts must be in reasonable proportion

to the seriousness of the violated interest and to the intended effect of the penalty. At that last one

It is important that a penalty must provide such an incentive that the order is complied with.

58. If the NP does not end the observed violations within six months, it will forfeit a

penalty. The AP sets the amount of this penalty at € 12,500 for each week that the order is not

(in full) has been carried out up to a maximum of € 200,000. In the opinion of the Authority, the

amount of these amounts in reasonable proportion to the seriousness of the violation caused by the violation

interest - the protection of police data and the privacy of those involved - and

are these (further) sufficiently high 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

Operative part

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

The NP must be submitted within six months of the date of this decision in the context of data processing

take measures in N.SIS II that lead to:

i.

the NP establishes a procedure that relates to authorizations for the business information managers

of the parties affiliated to N.SIS II and the employees of the IND who, within the framework of N.SIS

II process personal data;

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

of persons authorized to view and edit personal data in N.SIS II

process;

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

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

IND employees;

changed authorizations are logged;

the log files are regularly proactively checked for indications of wrongdoing

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

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

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

two hundred thousand euros).

Yours faithfully,

Authority for Personal Data,

e.g.

Mr. A. Wolfsen

Chair

Remedies

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

decision 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 is responsible for supervising the processing of

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

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, conduct an investigation into the

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

under the law.

2. The Board will 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 whom it concerns.

[…]

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

1. The members and extraordinary members are responsible for supervising compliance as referred to in Article 51, first

paragraph

members of the Board, the civil servants of the secretariat of the Board, as well as those appointed by decision of the Board College Designated Persons.

[…]

4. The Board is authorized to impose an order under administrative coercion to enforce Section 5:20, first paragraph, of the General Administrative Law Act, insofar as it concerns the obligation to provide cooperation with a civil servant designated by or pursuant to the first paragraph.

[…]

Article 65 of the Wbp:

The Board is authorized to impose an administrative coercion order to enforce the at or obligations under 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.

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 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 6 of the Wpg (insofar as relevant)

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

2. Police data will only be processed by police officers authorized by the
responsible are authorized and insofar as the authorization extends.

3. The responsible party authorizes the police officers under its management for the
processing of police data for the performance of 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
official is authorized and the parts of the police task for 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 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.

Date

February 6, 2017

Our reference

z2015-00910

Police information security regulation (Rip)

Article 2, first paragraph, of the RIP:

1. These regulations apply to the entire process of information provision and the entire

life cycle of information systems, regardless of the technology used and regardless of the character of the

information.

Article 3(1) and (2) of the RIP (where relevant):

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

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

investigation of criminal offences, the Chief of Police adopts this policy document after consultation with the Chief Public

Prosecutor

of justice.

2. The document includes at least:

[…]

f. the manner in which detected or suspected breaches of information security are passed on

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

how they 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, which system of information security measures is determined

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

[…]

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

is determined. In any case, this includes:

1. an action plan to implement all security measures;

2. a calamity section, the effectiveness of which is tested periodically.

Police Act 2012

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

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

a. […]

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

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 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,

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

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

on access to the data);

g) it is ensured that all authorities with a right of access to SIS II or facilities for

data processing, drawing up profiles describing the tasks and responsibilities

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

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

national supervisory authorities referred to (staff profiles);

[…]

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 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.

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, opening words, of the Decree refers to a security plan, while Article 10, first paragraph, opening words of the Regulation

talks about a safety plan. These terms mean the same thing.

Date

February 6, 2017

Our reference

z2015-00910

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

to fulfill their duties under this Regulation.

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.