ROYAL NORWEGIAN MINISTRY
OF LABOUR AND SOCIAL INCLUSION

EFTA Surveillance Authority
Avenue des Arts 19H
1000 Brussels
Belgium

Your ref	Our ref	Date
	22/3509-	4 November 2022

Reply to ESA concerning the Norwegian Labour and Welfare administration's processing of IP addresses

Introduction

Reference is made to your letter of 31 August 2022 where the Internal Market Affairs Directorate (the Directorate) of the EFTA Surveillance Authority (ESA/ the Authority) informed of an own initiative case to investigate the application of Regulation 2016/679 (EU), the General Data Protection Regulation ("GDPR"), as well as its predecessor, Directive 95/46/EC in Norway from 2012 until the present day. The case concerns the Norwegian Labour and Welfare Administration's processing of IP addresses, and the Norwegian Government has been asked to reply to twelve questions in this regard. The Norwegian Government's answers to the Authority's questions are based on available documents and information from the Norwegian Labour and Welfare Administration (NAV).

On 28 October the Ministry of Labour and Social Inclusion, the Ministry of Foreign Affairs and the Labour and Welfare Directorate met with representatives of the Authority to give a preliminary response to the questions regarding NAV's processing of IP addresses. In this meeting the Authority granted our request for an extension of the deadline, and we would like to thank the Authority for your understanding in this matter.

Recipients of work assessment allowance and unemployment benefits are required to send an employment status form (meldekort) every fourteen days as a condition for receiving the benefit. NAV collected information about IP addresses and used it to identify whether the recipient was located in Norway or abroad. In the introduction to the Authority's request, reference is made to the wrongful application of EEA law in relation to the export of sickness benefits and work assessment allowance.

Postal address	Office address	Telephone	Department	Reference
Postboks 8019 Dep 0030 Oslo postmottak@aid.dep.no	Akersgata 64 www.aid.dep.no	+47 22 24 90 90 Org. nr. 983 887 457	Budsjett- og styringsavdelingen	Jens Sandbrekke Wolther +47 22 24 86 42

Before going into the detailed responses to the Authority's questions, we will summarise the most important aspects of NAV's collection and storing of IP addresses from 2012 to the present day. Up to 11 March 2018 NAV had legal basis, both for collecting IP addresses and using the information for control purposes. The legal bases for the collection and sharing were the Personal Information Act of 2000 section 8 (f) and the National Insurance Act section 21-4, respectively.

In the period between 12 March 2018 and 11 September 2019 NAV collected the IP addresses of 495 229 persons, without having a legal basis for the collection. Among these, there are six cases in which IP addresses acquired without a legal basis were shared with the police. NAV's assessment is that the sharing of these IP addresses did not have any significance for the outcomes of the six cases. For the large number of persons who had their IP addresses collected, we assess that they have not suffered a breach of confidentiality, as the information was not shared with any third parties.

NAV sent 1700 appeals, where IP addresses may have been part of the case, to the National Insurance Court in the period from March 2018 to August 2019. There are currently no indications that IP addresses acquired after 11 March 2018 have been shared with the National Insurance Court. If NAV are to ascertain whether IP addresses have been shared with the National Insurance Court in these cases, NAV would need to review the 1700 cases manually. There are no plans for devoting resources to such a work intensive review of cases.

Answers to the Authority's questions regarding NAVs processing of IP addresses

Question 1

> *The Directorate understands that IP addresses were collected and retained when persons sent in their employment status form, and that these addresses were used for control purposes. Was this the sole purpose for which these addresses were used, and what was the legal basis for such processing, under Directive 95/46/EC, and under the GDPR?*

NAV collected and retained IP addresses when persons sent their employment status form. These addresses were later used for control purposes. The original purpose for collecting the IP addresses was security purposes in order to prevent unauthorised use of NAV's information systems. Important considerations with regards to information security and employment status forms were verification of the alleged recipient and prevention of attempts at unauthorized use.

The decision to collect IP addresses for security purposes can be traced back to a judicial assessment of employment status forms made back in 2001. At the time the processing of unemployment benefits was done by the Norwegian Labour Administration (Aetat). In the original assessment it was thought that collection of IP addresses could be used to identify the data subject sending the employment status form. With the benefit of hindsight we can

say that IP addresses does not help in this task. We would, however, like to stress that there has been significant technological progress since 2001 with regards to information technologies. There has also taken place a significant development with regards to the legal regulation of information collected through such technologies, perhaps most importantly the GDPR introduced in July 2018. In evaluating decisions made back in 2001 we should take into account the technological landscape, as well as the knowledge and understanding of data protection at that time.

The legal basis under Directive 95/46/EC was the provision of section 8 (f) of the Personal Data Act of 2000. Section 8 (f) stated that personal data may be processed if the processing was necessary in order to enable the controller or third parties to whom the data are disclosed, to protect a legitimate interest, except where such interests are overridden by the interest of the data subject. The provision assumes that the data controller has made this balancing of interests prior to the processing. Whether section 8 (f) of the Personal Information Act of 2000 can be used as a legal basis for processing IP addresses for security purposes was dealt with by the Privacy Appeals Board in 2009 and 2014. In both decisions, the Privacy Appeals Board stated that the processing of IP addresses had to be considered a necessary security measure and that the processing did not represent a disproportionate invasion of privacy of the data subjects. The Privacy Appeals Board concluded that there was a basis for processing according to Section 8 (f) of the Personal Data Act, even if no assessment was made as to whether the conditions in 8 (f) had been met prior to the processing of the personal data.

These decisions are also supported by a judgement in the EU Court from 2016 (Case C-582/14).The court stated that the Federal German institutions may have a legitimate interest in storing the IP addresses in order to protect the institution's website against cyber-attack.

Regarding the current legal basis for processing IP addresses in accordance with the GDPR, NAV concluded in May 2019 that there is no legal basis for processing IP addresses according to the rules of the GDPR.

Question 2

> *For how long were IP addresses stored, and what was the legal basis for their storage? How was this time limit determined?*

The IP addresses were to be stored for ten years after delivery. In practice, NAV did not comply with this as IP addresses were not deleted between 2005 and 2019. In September 2019 all IP addresses were deleted. NAV’s purpose of continued storage was based on archival purposes in the public interest in accordance with the provisions on archival material in the Archives Act. Such further processing is compatible with the original purpose, cf. Article 5 (1) (b) of the General Data Protection Regulation.

Question 3

Was the purpose for which the data was collected specified before the data was collected? Was this made clear to the data subjects? If so, how was this done? What information was provided to the data subjects?

The purpose of security was specified before the data was collected. No specified information was provided to the data subjects about the purposes of collecting the data. It was not necessary to provide this information under the Personal Information Act of 2000, as the sole use of information about the electronical trace was in technical processes.

Question 4

Was the data then used for any purpose beyond the original purpose for which it was collected?

Some of the data was also reused for control purposes. The legal basis for control purposes was section 21-4 of the National Insurance Act. According to section 21-4 first paragraph, NAV can obtain information that is necessary to control if the conditions for a benefit are being met, or have been met in previous periods. The Norwegian Labour and Welfare Administration thus assessed that NAV had a legal basis for processing IP addresses for control purposes until 11 March 2018.

There is a distinction to be made between the *collection* of IP addresses, which had legal basis in the Personal Information Act of 2000, and the *sharing* of information for control purposes, which still has a legal basis in the National Insurance Act section 21-4. The Personal Information act of 2000 has been replaced by the GDPR. The National Insurance Act section 21-4 can still be used as a legal basis for sharing information for control purposes. It is the *collection* of IP addresses that no longer have any legal basis.

The data was not collected for control purposes. However, some of the collected data was reused for control purposes. Even though the data subjects were not informed about this at the data collecting time, there was a legal basis for collecting and reusing the data until 11 March 2018.

Question 5

How are such communications presently treated? Are IP addresses still processed or stored? If so, what is the legal basis for this?

The reuse of IP addresses stopped in May 2019, and all IP addresses were deleted in September 2019.

Question 6

The Directorate understands that, until 11 March 2018, it was possible to log into the system with a username and password, but that since 11 March 2018, it has only been possible to access the system with MinID, BankID, Commfides or similar two-

factor authentication keys. Were IP addresses of users still processed and/or stored after this date? If so, what was the legal basis for this processing and/or storage?

Until 11 March 2018, it was possible to log into the system with a username and a password. After 11 March 2018, when users could only log in to their personal NAV page (Ditt NAV) via the ID port, there was no longer a need for IP addresses as a security measure to prevent unauthorized use of information systems. The Norwegian Labour and Welfare Administration therefore concluded in June 2019 that NAV had no legal base under the Personal Data Act of 2000 section 8 (f) to continue to process IP addresses after 11 March 2018. After the New Personal Data Act and the GDPR came into force on 20 July 2018, public authorities no longer have a legal base for processing personal data based on legitimate interest, cf. GDPR article 6 no.1 letter f.

NAV's reuse of IP addresses ceased in May 2019, as part of a privacy consequence assessment for employment status forms. As part of the same process, NAV concluded in June 2019 that there was no legal basis for the collection of IP addresses.

Question 7

Did the practice change after the entry into force of the GDPR in the EEA on 20 July 2018? If so, what was the legal reasoning for the change?

The practice changed in May 2019. Please refer to our response to question six.

Question 8

Was the Norwegian Data Protection Authority ("DPA") informed about this practice? If so, when did this take place? Were data subjects notified individually at the same time as the DPA that their personal data had been processed, or was being processed, or were they informed at a later juncture? What information was conveyed to the DPA? What action, if any, was taken by the DPA?

The Norwegian Labour and Welfare Administration notified the Norwegian Data Protection Authority about this practice via Altinn in March 2022. In the web service Altinn, the notification was fully signed, but not transferred, so NAV does not know with certainty at what date the DPA received the notification. NAV resent the notification in Altinn on 6 October 2022.

The DPA was informed that a lack of legal basis led to an erroneous disclosure of personal data to the police in the period from 12 March 2018 until 6 May 2019. During this period NAV has provided IP addresses to the police as documentation of incorrectly paid benefits in six cases where the user stayed abroad while receiving unemployment benefits or work assessment allowance. Disclosure of the IP addresses is a breach of confidentiality. This discrepancy was not notified to the DPA earlier because the Norwegian Labour and Welfare administration at first primarily considered that the discrepancy was a matter of a lack of legal basis, with little practical significance for the data subjects.

The data subjects were not notified individually. The Labour and Welfare Directorate assessed that the breach was not likely to result in a high risk for the rights and freedoms of persons, according to article 34 of the GDPR. They assessed that NAV's measures to notify the police about a lack of authorization for IP cases meant that the breach no longer entailed a risk for the rights and freedoms of the data subjects that were affected.

Question 9

Approximately how many persons are affected by the processing of their personal data in this manner?

The Labour and Welfare Directorate considered that the breach of confidentiality only applies for IP addresses collected and disclosed to the police after 11 March 2018. There are six persons who are affected by NAV's disclosure of IP addresses to the police.

Question 10

Approximately how many (formal or informal) enquiries and complaints have been received in relation to this issue by the Norwegian Government and/or the NAV? Please summarise the main lines of complaint received.

It has not been possible to obtain specific figures on the number of complaints or enquiries concerning IP addresses. It is assumed that most of the complaints NAV has received regarding IP addresses have been directed at the various administration units in connection with reimbursement request payment. NAV Kontroll which has processed IP addresses in connection with suspected social security fraud, has informed that they received a couple of enquiries about the use of IP addresses in their cases. This was after a media report in the online newspaper E24 in the spring of 2021.

Question 11

Have any remedies been made available to those whose personal data was processed? How can these remedies be accessed? How does the Norwegian Government intend to quantify damage?

In all decisions where the IP addresses have resulted in a case for refusal /repayment, the data subject is informed in the decision letter about the right to appeal the decision. In those cases where NAV provided IP addresses to the police as documentation of incorrectly paid benefits we assume that the principle of contradiction has been adequately safeguarded both through notification and decisions in the provision. In the six cases reported to NAV after 11 March 2018, we have been informed that only one has been sentenced to unconditional imprisonment, one has been acquitted and one has been dismissed by the police, the rest have been suspended by the police. In the case with an unconditional prison sentence, NAV's assessment is that the IP address had no significance for the outcome of the criminal case, as the IP addresses for the reported and convicted period were collected before 12 March 2018.

NAV sent a letter to the police in five cases in 2019 in which they informed about the lack of legal basis and asked the police to disregard the IP addresses collected after 11 March 2018. A similar letter was sent to the police in one case in 2021.

Question 12

Has any litigation been initiated by any affected parties, specifically in relation to data protection issues arising from the NAV's processing of IP addresses?

We are not aware of any litigation by the affected parties in relation to protection issues arising from NAV's processing of IP addresses.

Yours sincerely

Camilla Landsverk
Deputy Director General

Jens Sandbrekke Wolther
Adviser

This document is signed electronically and has therefore no handwritten signature