The Swedish Migration Agency

Slottsgatan 82

602 22 Norrköping

Diary number:

DI-2019-13667

Your diary number:

1.3.3-2019-43845

Date:

2021-11-17

Decision after supervision according to

data protection regulation –

The Swedish Migration Agency's treatment of

personal data in VIS

Content

Mailing address:

Box 8114

104 20 Stockholm

Website:

www.imy.se

E-mail:

imy@imy.se

Phone:

08-657 61 00

4.

1. The Data Protection Authority's decision

The Privacy Protection Authority issues warnings, with the support of 58.2 a

data protection regulation, as the Migration Agency's processing will likely break

against the provisions of the data protection regulation as follows.

1. The continued development and management of the VIS may, contrary to Article 32

the data protection regulation, may be compromised due to ambiguities around

The status of the IT documentation, which may lead to the Migration Agency not taking action

appropriate technical and organizational measures that ensure a

security level that is appropriate.

2. Data in user logs may, in violation of Article 5.1 e

the data protection regulation on storage minimization, will be saved under a

longer than is necessary for the purposes for which

the personal data is processed, because the Swedish Migration Agency lacks a routine for

thinning of user logs.

2. Statement of the supervisory matter

2.1 Purpose and scope of the review

The Privacy Protection Agency (IMY) has, in accordance with the established inspection plan

reviewed the Swedish Migration Agency's processing of personal data in the national part of

the Visa Information System (VIS). The purpose of the review has been to

check whether the processing of personal data is in accordance with the applicable

right, i.e. The VIS Regulation1 and the Data Protection Regulation (GDPR)2.

IMY has an obligation according to Article 41.2 of the VIS Regulation to review the processing i

the national part of the VIS at least once every four years. The review shall

conducted in accordance with international accounting standards.

During the review, IMY has asked questions regarding the processing of personal data in VIS,

personal data responsibility, personal data assistants, competent authorities,

information exchange with other member states, thinning, transfer of personal data

to third countries, rights of data subjects, training of personnel and IT security.

1 REGULATION (EU) 767/2008 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 9 July 2008 on

the Visa Information System (VIS) and the exchange between Member States of information on visas for shorter

stay (VIS regulation)

2 REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the

protection of

natural persons with regard to the processing of personal data and on the free flow of such data and on

repeal of Directive 95/46/EC (General Data Protection Regulation)

2.2 Implementation and method

IMY has on three occasions, on 16 January 2020, on 21 February 2020 and on 5 October

2021, on site at the Swedish Migration Agency reviewed the processing of personal data in it

the national part of the VIS. The Swedish Migration Agency has, on the first occasion, shown the VIS and they

the national IT systems Wilma, W2, VIS-mail and the central alien database

(CUD).

After the first inspection, IMY has sent a number of written questions

The Swedish Migration Agency, which the agency has answered before the second inspection.

On the second inspection occasion, IMY asked supplementary questions and carried out

random checks of completed visa cases in Wilma as well as ongoing ones

visa cases in W2.

Due to the pandemic, it has the third inspection opportunity, focusing on

user logs, had to be postponed until autumn 2021. Before this occasion, IMY has sent a

number of supplementary questions that the Migration Agency has had to answer.

On the third inspection occasion, IMY reviewed the user logs and asked

supplementary questions. The Swedish Migration Agency has also been given the opportunity to inform about what

which may have changed since inspection 2.

2.3 About VIS

VIS is an EU joint system for the exchange of information on visas for shorter ones

stays between EU member states. The purpose of VIS is to facilitate the procedure at

visa applications, prevent a circumvention of the rules on which member country

responsible for examining a visa application, facilitating the fight against fraud,

facilitate checks at border crossings at the external borders of Schengen and

within the territory of the Member States and to contribute to the prevention of threats to

internal security of the Member States.

VIS contains personal data collected and registered in connection with

visa application. Which personal data may be processed is specified in the VIS regulation

and includes i.a. fingerprints and photographs.

The Swedish Migration Agency is appointed to be responsible for personal data according to Article 41.4 of the VIS-

the regulation for Sweden's processing of personal data in the VIS. Personal data responsibility

also includes the foreign authorities' automatic processing when handling

visa applications. Other, specially appointed, authorities also use VIS, e.g. in it
law enforcement activities.

The main component of the IT system is the central database (C-VIS), which contains
information on visa applications and decisions from the member states. The central one
the database is managed by the European Agency for the Operational Management of Large IT
system in the area of freedom, security and justice (eu-Lisa). There is also one
integrated communication system, ViSMail, which is used for communication between
Schengen states in current and completed visa cases.

Each member state has national systems (N-VIS) that communicate with it
central database. In Sweden, the Migration Agency uses the process-based system
the case management system W2 to manage ongoing visa applications and Wilma

to handle closed cases. National information is stored in the central
the Aliens Database (CUD).

3. Justification of the decision

3.1 What the review covered

IMY's review has covered which personal data is processed in the national
part of the VIS, who is the personal data controller for the processing, if there is one
personal data processors and the conditions for how they process personal data,
who are the competent authorities and what data they have access to, how
the exchange of information with other member states is for, how long personal data
saved in the national part, how data quality is ensured and record keeping
works, if the data is transferred to third countries, how the rights of the data subjects

is ensured, which training in the handling of personal data is provided
the staff and how IT security works. Section 3.9.1 shows in more detail what
included in the review of IT security.
During the justification of the decision, IMY addresses selected parts of what was reviewed. IN
otherwise, IMY has no views on the treatment.

3.2 The VIS Regulation in relation to the Data Protection Regulation

The Data Protection Regulation was introduced on 25 May 2018 and is the primary legal one
the regulation when processing personal data.
The provisions of the Data Protection Ordinance apply to the extent that there is no special regulation
in the VIS regulation. This is apparent from recital 17 in the VIS regulation and article 94.2 i
data protection regulation.

3.3 Basic conditions for processing personal data in VIS

3.3.1 The Swedish Migration Agency's purposes for the processing of personal data in the VIS

Article 2 of the VIS Regulation specifies the purposes for which personal data may be processed.
For the Swedish Migration Agency, it is primarily about managing and deciding on
visa cases. Nothing has emerged within the scope of the review and those
random checks carried out by IMY which indicate that the Migration Agency would process
data in the national systems for purposes other than what appears in the VIS
the regulation.

3.3.2 Data that may be processed according to the VIS regulation

In the VIS regulation, there are several articles (articles 9-14) which explicitly state
which information may be processed in connection with a visa application.
IMY has reviewed which information has been registered in Wilma and in W2. In very large
to an extent, the categories of tasks are predefined, i.e. there is a very little
space for a person with access to the systems to process other categories of

data in the national systems. The IMY's spot checks have also not shown that

The Swedish Migration Agency would process data other than what the authority has support for

process according to the VIS regulation.

3.4 Personal data responsibility

According to Article 41.4 of the VIS Regulation, each Member State must appoint an authority which

shall be the personal data controller and have central responsibility for this Member State's

processing of data. The Swedish Migration Agency is the nationally designated authority,

which appears from § 11 point 3 regulation (2019:502) with instructions for

The Swedish Migration Agency.

Section 9 of the Aliens Data Act (2016:27) also states that the Swedish Migration Agency is

personal data controller for the authority's processing of personal data. In addition, is

According to the aforementioned provision, the Swedish Migration Agency is also responsible for personal data

the foreign authorities automated processing of personal data, which includes

processing of personal data in the VIS.

In the case, the Swedish Migration Agency has, among other things, informed that full-time employees at

foreign authorities, which handle migration matters, since 1 January 2020

employees of the Swedish Migration Agency, while part-time employees and local employees as well

continue to be employed by the Ministry of Foreign Affairs (MOF). Employees at UD i

Stockholm does not handle migration cases at all and does not have any

access to the VIS system. In order to clarify the relationship of responsibility between

An administrative agreement has been signed between the Migration Agency and the Foreign Ministry

the parties.

IMY sees positively that the Swedish Migration Agency and the Foreign Ministry have signed an agreement management agreement. It is important that the borders of the Swedish Migration Agency responsibility for personal data is clarified in relation to the Ministry of Foreign Affairs. IMY has no views on what which emerged in the case regarding personal data responsibility.

3.5 Processing of special categories of personal data

IMY has specifically asked questions about the Migration Agency's processing of fingerprints and photographs. Article 9 of the VIS regulation states that the visa authority must register both a photograph of the applicant and fingerprints. The Swedish Migration Agency has described how fingerprints and photographs are recorded and managed and how the quality on the data is ensured.

The Swedish Migration Agency has informed that nothing is being asked from the EU level explicit demand for the quality of a fingerprint and explained that it probably depends on that it is better to have incomplete or to some extent "worse" imprints in the central VIS none at all. However, there are requirements for dissolution and certain other requirements in (2009/756/EC), which is referred to in "Appendix guidance for processing visa applications and change of issuing visas" (Guide I on the Visa Code). Instead have it called on Member States to ensure that they are really trying to achieve the best possible quality by measuring at the time of recording and, if possible, applying the same algorithm for measuring quality during recording that is used centrally at storage. The quality is measured during storage and the Member States are provided with statistics on what has been achieved quality on an aggregated level.

The Swedish Migration Agency has informed that the authority has chosen to use the same quality software for fingerprints used in the central VIS in the biometrics stations the authority uses. Using this software is measured the recording of individual fingers and also the sum of all fingers on a hand according to

a weighting. The operator is prompted to redo the impressions if the quality is low and

6(10)

can also choose to use the best finger if multiple recordings are made, all on purpose

to send the best possible impression to the central VIS. Follow-up of quality on

recordings are made to ensure that the prints sent to VIS keep a pile

quality, one factor is the training/motivation/skill of the operator. Other important

factors are the age of the third-country national, occupation, ethnicity and individual differences

of a different species. According to the Swedish Migration Agency, the authority has ensured that the equipment is off

good quality, that the process of recording is good and that the measurement of fingerprints

quality is done and followed up.

IMY makes the assessment that the Swedish Migration Agency has taken adequate measures to

ensure a good quality of the fingerprints registered by Sweden in the VIS and

the handling therefore does not cause any comments from IMY.

3.6 Deletion of information in the VIS when the court has changed a previous one

rejection decision

Article 25.3 of the VIS regulation states that if an application for a visa is rejected

has been annulled by a court or appellate body, the Member State which refused

application delete the data referred to in Article 12 of the VIS Regulation as soon as the decision

to revoke the refusal has gained legal force.

The Swedish Migration Agency has initially stated that there is a developed manual routine for monitoring

that an application is deleted in accordance with Article 25.3 of the VIS Regulation but that at

the authority's control revealed that the routine was not always followed. In September 2021 have

The Swedish Migration Agency supplemented with information that there is already one

function in W2 where decision-makers at the immigration authorities can remove a decision from C-WAY. The Swedish Migration Agency has now clarified the routine for how this function should be used in in accordance with Article 25.3 of the VIS Regulation. The Swedish Migration Agency has also produced one proposals for how the removal can be automated and informed that the IT development required to introduce the automation is expected to be completed in Q1 2022.

IMY sees positively that the Swedish Migration Agency has clarified the manual procedure for deletion according to Article 25.3 of the VIS Regulation and the plans to develop an automated routine and has no views on the handling.

3.7 Thinning of data in the national information systems

3.7.1 Data in the national systems

According to the data protection regulation, see articles 5.1 b, 5.1 e and 89.1, there are possibilities to save data for archival purposes with the support of national regulations. One According to the Archives Act (1990:782) and the Archives Ordinance (1991:446), the authority is obliged to keep their public documents and may only, according to § 14 of the Archives Ordinance, file these in accordance with regulations or decisions of the National Archives, unless special thinning regulations are in law or regulation.

From the appendix to the National Archives' regulation RA-MS 2013:45 section 5.2.1.6 it appears that The Swedish Migration Agency may file documents in visa cases five years after the decision date According to the Swedish Migration Agency, the authority ensures, both through automatic thinning and manual procedures, that documents are deleted in national information systems. According to The Swedish Migration Agency thins out data from the national operational systems after six years. It is the visa documents that are being thinned. Certain information, such as personal information and

overall information, is transferred to a national e-archive, which is a separate database
separated from the national operational systems. If there are multiple cases connected
an individual is thinned when the thinning deadline has expired for all visa cases.
The Swedish Migration Agency has stated that the reason for data being thinned out after six years and not
five years after the date of the decision, which the thinning regulation allows, is a business reason.
IMY has no views on what emerged in the case regarding how
The Swedish Migration Agency sifts visa data and transfers data to the e-archive.

3.7.2 Data retrieved from C-VIS

Data stored in the national system can either be data that
retrieved from the central database C-VIS and entered by other Member States
or information entered by Sweden.
Article 30.1 of the VIS regulation states that data from C-VIS may only be saved in one
individual case as long as it is necessary in accordance with the purposes of VIS and i
in accordance with applicable legal provisions. It is clear from Article 30.2 that it is not
affects the Member States' right to store data that they have entered into the VIS in their
national information systems. Any use that is not compatible with points 1
and 2 shall, according to 30.3 VIS regulation, be considered abuse according to each
Member State's national legislation.
According to the Swedish Migration Agency, no data retrieved from C-VIS is saved in the national data
systems in addition to the VisMail correspondence that may exist in individual visa
and/or asylum cases. These data are processed at the same time as the case in its entirety
thinned according to national thinning rules.
IMY has no views on the handling.

3.8 Training of personnel at the foreign authorities

During the ongoing supervision, the Swedish Migration Agency has put into operation an interactive
data protection training for employees. It is provided to the staff at

the foreign authorities and at the Swedish Migration Agency who work in the VIS. The education has has been available since the end of 2020. A follow-up of who has completed the training is planned as an activity for next year. The Swedish Migration Agency's data protection officer has responsibility for follow-up.

IMY sees positively that the Swedish Migration Agency has developed an interactive training course and has none points of view.

3.9 VIS and IT security

3.9.1 What the review of IT security covered

The Swedish Migration Agency has described the routines for authorization allocation, identification of users, documentation of the IT architecture, password change policy, controls of permissions, the management of user logs and data quality reviews.

3.9.2 Applicable Regulations

The basic principles for processing personal data are set out in Article 5 data protection regulation. A basic principle is the requirement of security according to Article 5.1 f, which states that the personal data must be processed in a way

which ensures appropriate security for the personal data, including protection against unauthorized or unauthorized processing and against loss, destruction or damage by accident, using appropriate technical or organizational measures.

From Article 5.2 of the data protection regulation, the so-called the liability, i.e. to the personal data controller must be responsible for and be able to demonstrate that the basic the principles in point 1 are complied with.

Article 32 of the data protection regulation regulates security in connection with processing.

According to paragraph 1, the personal data controller shall, taking into account the most recent
the development, implementation costs and the nature, scope,
context and purpose as well as the risks, of varying degree of probability and seriousness,
for the rights and freedoms of natural persons, take appropriate technical and
organizational measures to ensure a level of security that is appropriate i
relation to the risk (...). According to paragraph 2, when assessing the appropriate
security level special consideration is given to the risks that the treatment entails, in particular
from accidental or unlawful destruction, loss or alteration or to unauthorized disclosure of
or unauthorized access to the personal data transmitted, stored or otherwise
treated.

In Article 32.2 of the VIS Regulation, more detailed IT security requirements are specified in this regard
national interface. Although the article according to the wording of the article is aimed at
Member States provide guidance in the interpretation of Article 32
data protection regulation of the requirement to take appropriate technical and organizational measures
measures to ensure a level of security that is appropriate in relation to the risk.

The Swedish Migration Agency is responsible for personal data for VIS in Sweden and is thus the one
authority that is ultimately responsible for ensuring that the requirements of Article 32 of the Data Protection Regulation and
32.2 of the VIS regulation are fulfilled.

3.9.3 Documentation of the IT architecture over VIS

Correct and up-to-date documentation of the IT architecture is an important part of that
protect the information and IT systems and reduce risks and vulnerability, e.g. when staff
replaced or discontinued. It is such an organizational measure as is required under Article 32
data protection regulation.

On one inspection occasion, the Swedish Migration Agency handed over a document of IT-
the architecture of the VIS which, according to the authority, was not completed. At the time of inspection
three, the Swedish Migration Agency has submitted an updated version, prompted by a project

with the aim of adapting the architecture to a future EU system. The updated
version of the document reflects, according to the Swedish Migration Agency, the appearance of it
the national part of VIS has right now, but the project will mean that the structure is made
if.
The latest version of the document that IMY has seen has the status "draft"
stated in the document and there is no decision date in the box "decided by" and
information in the "approved by" box. According to the document history, it was last updated
on 3-4 February 2020.
IMY does not question the Swedish Migration Agency's statement that the document is updated and
reflects the current IT architecture. However, there is no information in the box
“approved by” and the date of approval box, which could mean that
the document is not formally decided by the authority. It is not clear to it either
who reads the document that it is up-to-date and reflects current IT architecture.

According to IMY, it is likely, due to the uncertainty surrounding the document's status for
the reader, that inaccuracies may occur in the development and management of VIS, which i
in turn may lead to the Migration Agency not taking appropriate technical and
organizational measures that ensure an appropriate level of security in accordance with Article 32
data protection regulation.
3.9.4 Logging of user activities and log follow-up
Article 32.2 of the VIS Regulation states that each Member State shall, with regard to
its national interface, take the necessary measures, including adopting a
data protection plan, to ensure that it is possible to verify and determine which

information that has been registered in the VIS, when this has been done, by whom, and for what purpose (control of data registration).

The Swedish Migration Agency has described how the logging of user activities is done. IMY has also on the occasion of inspection three reviewed which information has been registered in the user log regarding two completed visa cases.

The Migration Agency's information and IMY's random check show that it can be verified and determine what information has been registered in the VIS, when this has been done, by whom, and for what purpose. Against this background, IMY has no views on the logging of user activities.

3.9.5 Thinning of user logs

A user log that is saved longer than is necessary for the purpose can itself pose a security risk. In the assessment, according to Article 32 of the Data Protection Regulation, of appropriate security measures and user logs is to decide how long there is a need to save these from an IT security perspective. According to the principle of storage minimization in Article 5 c of the data protection regulation, personal data shall not stored longer than is necessary for the purpose.

According to the Swedish Migration Agency, the user logs must be thinned after 10 years, which corresponds to the statute of limitations for serious data breaches. At inspection 2, the Migration Agency stated that the authority has not yet started any routine for thinning user logs. IMY has then requested information on how old the oldest log entry is and received a response from The Swedish Migration Agency that it was registered on 2012-09-01.

On existing basis, IMY does not question the chosen time period to save logs.

IMY notes, however, that the choice of time period seems to be primarily based on one information security perspective and not an integrity perspective and therefore wants to underline that both perspectives must be taken into account in the assessment.

Furthermore, IMY can state that there has not yet been any thinning of user logs,

which is explained by the fact that the oldest log entry was registered a little over nine years ago

i.e. the time for thinning has not yet passed. A lack of a routine for thinning out

user logs can, now that the time to start thinning logs is approaching, likely

lead to incorrect processing of personal data, i.e. that data in user logs

is saved for too long in violation of Article 5 e of the data protection regulation.

4. Choice of intervention

4.1 Legal regulation

The IMY has a number of corrective powers available under Article 58(2).

data protection regulation. If a treatment is likely to infringe

the provisions of the data protection regulation or supplementary statutes may IMY

according to article 58.2 a of the data protection regulation, issue a warning.

Other corrective measures in Article 58.2 b-j, i.e. above all reprimand, injunction

or administrative penalty fees, assuming that IMY has determined that it

personal data controller processes personal data in violation of

the data protection regulation or supplementary statutes.

4.2 The Migration Agency must be assigned two warnings

In sections 3.9.3 and 3.9.5, IMY has assessed that it is likely that the Migration Agency's

processing may lead to incorrect processing of personal data. It is not

question of established deficiencies that may lead to a reprimand, injunction or

administrative penalty fees. Otherwise, IMY has not established any violation

of the data protection regulation. It means that the corrective authority that is

possible for IMY to use within the scope of this supervision are warnings.

Both probabilities are of such a nature that, according to IMY, it is justified to assign one

warning that future treatments may be in conflict with Article 5 e

the data protection regulation and Article 32 of the data protection regulation respectively.

_____

This decision has been taken by unit manager Charlotte Waller Dahlberg after a presentation

by the lawyer Jonas Agnvall. In the final processing of the case has also

lawyers Lisa Zettervall and IT security specialist Johan Ma participated.

Charlotte Waller Dahlberg, 2021-11-17 (This is an electronic signature)

Copy to:

The data protection officer