EMN Ad-Hoc Query on NO AHQ on Use of Cloud Services for Processing Personal Data in Immigration Cases

Requested by Jolandie CLEMENTE on 17th January 2018

Miscellaneous

Responses from Austria, Belgium, Croatia, Czech Republic, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Slovak Republic, Slovenia, Sweden, United Kingdom, Norway (22 in total)

Background information:

Norwegian Authorities have started implementing digital services in the public sector. Many authorities have started using Cloud services, for economic and practical reasons. The Norwegian Directorate of Immigration (UDI) is considering the use of Cloud services for the processing of personal data in our ICT-systems. We would like to know whether and how other Member States are using or are considering the use of such services. Our questions are the following.

Summary

Of the 20 responding (member) states, only NO and DE indicated that they are considering the opportunities The Cloud presents in relation to processing immigration cases.

18 responding MS do not use, nor did they report plans of using The Cloud to store personal information for immigration case handling. In terms of having conducted any risk analysis, BE reported that the government had decided not to make use of The Cloud for immigration case work purposes.

LU reported that they had adopted a strategy for the use of Cloud technologies by its administrations in 2016 and that in the future, control of the risks connected with the use of Cloud services would be in the hands of a central service responsible for governance of The Cloud for government purposes.

Latvia uses self-maintained Cloud services to exchange information between different units of the organisation. NL reported that the government actively uses private cloud solutions though not for immigration casework. This means that the cloud 'infrastructure' is specially adapted for government actors' use. NL reported that an increasing number of government actors use these ‘private clouds’ collectively which they consider financially more efficient.

Questions about agreements etc. were not relevant for any of the respondents.

LU reported that the government bill n° 7184 introduced to Parliament (which will transpose Directive 2016/680/EU) will go into effect in May, so that it was too soon to do a risk analysis.

Questions

1. Are you using Cloud services for the processing of Personal data in Immigration Cases? Yes/No a. If yes: for all or only for special categories of personal data? Please specify:_____ b. If no, what are the main reasons?

2. If ‘yes’ to 1: a. Do you (intend to) have separate data processing agreements for such processing? Yes: ___ No: ____ b. If ‘yes to 2a: Was or will be the agreement with the supplier individually negotiated: Yes:___No: ___ c. If ‘No’: Do you (intend to) use standard data processing agreements? Yes: ____ No: ____
3. If you have individual data processing agreements: a. Have/will the agreements been negotiated on a central national level or individually for the Immigration authorities? Central level: ____ For the immigration authorities: ____ b. Are there significant differences between standard agreements and an individually negotiated agreement for the immigration authorities? Yes: ___ No: ____ If ‘yes’, what are the most important differences? Please specify: _____
4. Have you made Risk assessments when considering introducing Cloud services? Yes: ____ No: _____ If ‘yes’, which measures were considered or taken to ensure the protection of personal data and to demonstrate the compliance with the General Data Protection Regulation (GDPR)? Please specify: _____Would you be willing to share your Risk assessment or parts of it with the UDI? If ‘yes’, pleas provide a contact: _____

Responses

	Country	Wider Dissemination	Response
	Austria	Yes	**1.** No **2.** No, not at the moment **3.** N/A **4.** N/A ---------- Source: Ministry of the Interior
	Belgium	Yes	**1.** 1. In Belgium, the ICT unit of the Immigration Office does not store data on the “cloud”. The data are stored on servers administered by the Immigration Office/ICT itself. 1b. The main reason for not using cloud services is that the Immigration Office is willing to keep full control over security measures. Source: Information Security Advisor, Immigration Office

			2. N/A **3.** N/A **4.** To our knowledge, there is no formal or documented risk analysis from the Immigration Office/ICT regarding the use of cloud services. As the Immigration Office/ICT holds as a policy that the cloud shouldn't be used, no such analysis is planned. Source: Information Security Advisor, Immigration Office
	Croatia	Yes	**1.** No. **2.** N/A **3.** N/A **4.** N/A
	Czech Republic	Yes	**1.** No. To use the Cloud services is not the main priority of the Czech Republic and the Czech Republic doesn´t consider using it in the near future. **2.** N/A **3.** N/A (see Q1) **4.** N/A (see Q1)
	Estonia	Yes	**1.** No, in Estonia Cloud services are not used for the processing of personal data in Immigration cases. Data is stored in databases and their usage is regulated by law. Cross usage of data is performed via X-Road hence there is no need for Cloud usage. **2.** N/A

			3. N/A **4.** No.
	Finland	Yes	**1.** No b) Immigration matters and related personal data are classified as confidential data. Finland has a dedicated environment for this data. Traditionally the thought has been that this type is data is also saved into servers located in Finland. This makes it much more difficult to use cloud services for our services. **2.** N/a **3.** N/a **4.** N/a
	France	Yes	**1.** NO **2.** n/a **3.** n/a **4.** n/a
	Germany	Yes	**1.** No. BAMF is considering the opportunities for using Cloud services for the processing of Personal data in Immigration Cases. Future plans depend on certain conditions, e.g. legal regulations, technical feasibility, protection of data privacy, IT security and risk assessment. **2.** n/a **3.** n/a

			4. n/a
	Greece	Yes	**1.** NO. In Greece, the Directorate for E-Residence Permits (e-card) at the Ministry for Migration Policy does not store data on the cloud, while data (including biometrics) are stored on the servers of the Ministry for Migration Policy so that all necessary security checks are carried through only by the competent Directorate for e-Residence Permits. At the same time, Greek IT authorities have serious concerns on the security aspects of developping cloud services for residence permits. **2.** Not applicable **3.** Not applicable **4.** Not applicable
	Hungary	Yes	**1.** No. **2.** - **3.** - **4.** -
	Ireland	Yes	**1.** No. Ireland is not using cloud services for the processing of personal data in immigration cases. **2.** . **3.** . **4.** .

	Latvia	Yes	**1.** No, in general the Office of Citizenship and Migration Affairs and the State Border Guard is not using commercial Cloud services for the processing of Personal data in Immigration Cases at national level because of restrictions due to security and personal data protection reasons. However in some cases the Office of Citizenship and Migration Affairs is using self-maintained Cloud services to exchange information between different units of the organisation. **2.** No **3.** No **4.** No
	Lithuania	Yes	**1.** NO. According to Article 142 of the Law of the Republic of Lithuania “On the legal status of aliens”, the data related to aliens whose legal status in the Republic of Lithuania is determined under this Law and other laws of the Republic of Lithuania, legal acts of the European Union and international treaties shall be entered in the Register of Aliens. The data of the Register of Aliens shall be processed in compliance with this Law, the Law on Legal Protection of Personal Data and other legal acts, legal acts of the European Union as well as international treaties. Data has not been processed by using the solutions of private Cloud service providers due to yet unassessed risks. Such process would also require some changes in law. Current data processing in the Register of Aliens in itself does not mean that services of registers like Software as a Service (SaaS) could not be delivered while using Cloud solutions. Similar legal questions have been encountered when a foreign company applied to create and launch one such system for Police. National Data Protection Inspection was consulted about such possibility and the Inspection did not articulate categorical conclusion that SaaS services should not be delivered from a foreign provider. However, the Inspection shared some recommendations on the arrangements of additional agreements as well as legal acts in order to secure personal data protection. **2.** N/A

			3. N/A **4.** NO.
	Luxembourg	Yes	**1.** a. If yes: for all or only for special categories of personal data? Please specify:_____ b. If no, what are the main reasons? At the moment there has not been any discussion to introduce immigration cases in the cloud. Nevertheless, the Grand Duchy of Luxembourg has now adopted a strategy for the use of Cloud technologies by its administrations (23.12.2016). The transition of administrations to the Cloud offers undeniable advantages, and will indeed be essential for the future use of cutting-edge technologies (big data, machine learning, etc.). The Cloud will provide the administrations with access to a large catalogue of solutions, both for their own requirements and for services provided to the population. Solutions hosted in a Cloud can be deployed and implemented quickly. They are also extremely flexible in their use of resources, and reduce costs. Nevertheless, as soon as the use of a Cloud set up by another supplier becomes advantageous or indeed indispensable, it is important to ensure that the activity is properly supervised. In future, control of the risks connected with the use of Cloud services by the Grand Duchy's administrations will be in the hands of a central service responsible for governance of the Cloud for the requirements of the State's administrations and services. This central service will be tasked with advising and accompanying the Ministries and the State's administrations and services in their procedures for using Cloud services, supervising the State's use of the Cloud in order to detect possibilities for consolidation, and to ensure security and compliance with good practices and recommended frames of reference, particularly with regard to risk management. On 17 May 2017, the CSSF (Luxembourg Commission for the Supervision of the Financial Sector) published Circular 17/654 on IT outsourcing based on a cloud computing infrastructure. The circular intends to clarify the regulatory framework for recourse to cloud computing infrastructure supplied by an external service provider. Indeed, the circular reaffirms that CSSF considers that cloud computing is a form of outsourcing. The circular applies immediately to financial professionals, including credit institutions, investment firms, specialized PSFs, support PSFs, as well as payment institutions, and electronic money institutions. **2.** a. N/A b. N/A c. N/A

			3. a. N/A. b. N/A. **4.** N/A. 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 movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) will enter into force on 25 May 2018 and the government introduced bill n° 7184 to Parliament in order to transpose Directive 2016/680/EU so it is too soon to make risk assessments on data protection issues.
	Malta	Yes	**1.** NO The information systems related to the Immigration services and Border Control are property of the Malta Police and are physically hosted within the NS-SIS Unit datacentres. The main reason for such infrastructure emanates from the fact that in Malta the immigration authorities are part of the Malta Police. The Commissioner of Police is invested also to act as the National Principal Immigration Officer. **2.** No. c. Not in the very near future **3.** N/A **4.** N/A
	Netherlands	Yes	**1.** The Dutch Immigration and Naturalization Service (INS) currently does not use Cloud services for the processing of personal data in the ICT systems. It is not expected that public cloud services will be used any time soon to process such personal data. The Dutch government does use private cloud solutions. This means that the cloud 'infrastructure' is specially adapted for government actors' use. Currently, an increasing amount of government actors are using these ‘private clouds’ collectively (financially this is also more efficient). **2.** N/A **3.** N/A

			4. N/A
	Poland	Yes	**1.** No. Poland is not using Cloud Services for the processing of personal data in immigration cases. **2.** N/a **3.** N/a **4.** N/a
	Slovak Republic	Yes	**1.** N/A **2.** N/A **3.** N/A **4.** N/A
	Slovenia	Yes	**1.** No **2.** n.a. **3.** n.a. **4.** n.a.
	Sweden	Yes	**1.** No **2.** NA

			3. NA **4.** NA
	United Kingdom	Yes	**1.** No, the United Kingdom uses a secure Intranet to process personal data. The main reason for this is data security. **2.** N/A **3.** N/A **4.** N/A
	Norway	Yes	**1.** No, not currently We are planning for Cloud storage in the near future, and have seen several chalkenges, amongst these are; how to protect the storage of sensitive personal data in Immigration and Asylum cases; whether the terms and conditions of the Storage supplier are satisfactory and in line with Norwegian legislation and Data Protection regulations; and how to prevent the users from making wrong decisions when storing data. **2.** We are planning to use the Cloud Services provided by Microsoft. However, we intend to negotiate the terms and conditions in their Data Processing Agreeements. **3.** NA **4.** We are in the process of finalizing a Risk Assessment. Our preliminary Risk Assessment suggests several measures, such as: A classification of the information based on sensitivity, encryption of sensitive information, and restrictions on access and sharing of sensitive information with external or unsecured devices and user training. Yes, we are willing to share the results of the Risk assessments with others, at least in principle and at least in general terms. We will however have to consider how the information is shared within the agencies affiliated with

			the EMN Network. An option might be to share information within a meeting structure. The NO NCP is George Farnes, Data Protection Officer, gef@udi.no