# Annex: National Reports on the CEF cloud action

# Table of Contents

# AT SA

## Part I – Statistics

1. **Which stakeholders have you contacted under the coordinated action?**

- Federal Ministry of Education, Science and Research

2. **How many stakeholders have you contacted within the following categories?**

- Ministry of the central government: **One, see Q1.**
- Independent public body of the central government
- Buyer for the central government
- Publicly-owned company acting as a processor for several central public bodies
- Ministry of the regional government
- Independent public body of the regional government
- Buyer for the regional government
- Publicly-owned company acting as a processor for several regional public bodies
- Other, please specify

3. **How many stakeholders have you contacted within the following sectors?**

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government
- Economic affairs
- Education: **One, see Q1.**
- Finance
- Health
- Infrastructure
- Employment
- Justice
- Tax
- Other, please specify

4. **If you have contacted a buyer, for which sectors does this buyer provides its services?**

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government
- Economic affairs
- Education
- Finance
- Health
- Infrastructure
- Employment
- Justice
- Tax
- No specific sector
- Other, please specify

- **Answer:** N/A

5. **If you have contacted a buyer, please specify the number of stakeholders this buyer provides services for?**

- N/A

6. **What was the initial procedural framework of your action?**

– Fact finding
– Fact finding + determining follow-up action based on the results
– New investigation: **Started a new investigation**
– Ongoing investigation

7. **How many stakeholders indicated that they use CSPs or are planning to do so in the near future (end of 2022)?**

- One, see Q1.

8. **Of the stakeholders that use CSPs (or are planning to do so in the near future), how many use CSPs for the following functions?**

– Internal organisation (office suites, internal communication, HR, etc.) : **One, see Q1, in-house-Communication**
– Exercise of public functions (services to citizens, processing citizen's data, etc.): **One, see Q1, Communication**

9. **For the following commonly identified sectors, please specify if any hyperscalers are involved (if so please name them) - N/A**

– Health
– Finance
– Tax
– Education
– Central buyers or providers of IT services

10. **How many stakeholders took the following actions prior to- or during the acquisition of a CSP?**

– Perform a DPIA
– Does the DPIA analyses transfers in details (sometimes called DTIA)
– Perform a general risk analysis: **One, see Q1.**
– Contact the DPO for advice: **One, see Q1.**
– Contact the SA for advice

11. **How many stakeholders (including buyers) take the following actions during the use of the CSP?**

– Monitoring technical and organisational measures to ensure compliance
– In case of transfers, adopting technical and organisational measures, including supplementary measures, where needed, and monitoring if changes in the regulatory landscape occur (e.g. Schrems II): **One, see Q1**
– Regular risk assessments: **One, see Q1.**

## Part II – Substantive issues

1. **Pre-contractual phase**

**1.1. Briefly describe the main issue(s) identified.**

- Question whether DPIA would need to be carried out.

- Three offers have been evaluated esp. regarding the least processing of personal data required by the cloud provider

**1.2. Which provision(s) of the GDPR (or national laws) does this concern?**

- Art. 35 GDPR
- Chapter II

**1.3. Explain why this has been an issue for your stakeholders?**

- Public bodies feared questions of possible liability, even though they ultimately they deemed no DPIA to be necessary.

**1.4. What are differences that you have encountered between stakeholders in your Member State?**

- -

**1.5. What are solutions to this issue? Please describe if these solutions are already implemented or potential, and whether this solution is provided by the SA or the stakeholders.**

- Concerning Data Processing on this scale (eg. potentially more than 250 individuals concerned) a risk assessment should always be undertaken and properly documented (even if a DPIA is not legally required by the GDPR, in order to comply with Article 32 GDPR).

**2. Contract with the CSP**

**2.1. Briefly describe the issue (s0 identified.**

- Precise definition of the roles of the concerned parties.
- Applicable Law and court seat.
- Question how to ensure CSP acts only on behalf of and according to the documented instructions.

**2.2. Which provision(s) of the GDPR does this concern?**

- Art. 4 GDPR

**2.3. Explain why this has been an issue for your stakeholders?**

- Questions of liablility.

**2.4. What are differences that you have encountered between stakeholders in your Member State?**

- -

**2.5. What are solutions to this issue? Please describe if these solutions are already implemented or potential, and whether this solution is provided by the SA or the stakeholders.**

- The Controller has been advised to evaluate regularly whether agreement is kept and if necessary renegotiate.

**3. International transfers and access by foreign public authorities**

**3.1. Briefly describe the issue(s) identified.**

- Question of transfer of Personal Data taking place in the context of routine services provision and possible actions taken by controller to ensure the contractual obligations.

**3.2. Which provision(s) of the GDPR does this concern?**

- Chapter V GDPR, Art. 45 GDPR

**3.3. Explain why this has been an issue for your stakeholders?**

- Destination may fail to ensure essential protection. Controller had to contractually implement appropriate supplementary measures but follow-up assessments have not been conducted yet..

**3.4. What are differences that you have encountered between stakeholders in your Member State?**

- -

**3.5. What are the solutions to these issues? Please describe if these solutions are already implemented or potential, and whether this solution is provided by the SA or the stakeholders.**

- Even though follow-up assessments were deemed necessary, there were no actions or only little. The Controller has been advised to evaluate regularly.

**4. Telemetry data**

**4.1. Briefly describe the issue(s) identified.**

- Because of the applied hybrid operation, user content is processed locally and is not shared with the cloud/third countries.

**4.2. Which provision(s) of the GDPR does this concern?**

- Chapter II and V

**4.3. Explain why this has been an issue for your stakeholders?**

- Even though data protection risks with telemetry data were already public knowledge, stakeholders awareness during the pre-contractual phase was low. Stakeholders had only little to no precise knowledge about the processing, at first.

**4.4. What are differences that you have encountered between stakeholders in your Member State?**

- -

**4.5. What are solutions to this issue? Please describe if these solutions are already implemented or potential, and whether this solution is provided by the SA or the stakeholders.**

- Stakeholder has been advised to report follow-up assessments and measures taken.

**5. Compliance**

**5.1. Briefly describe the issue(s) identified.**

- Even though follow-up assessments were deemed necessary, there were no actions or only little. The Controller has been advised to evaluate regularly.

**5.2. Which provision(s) of the GDPR does this concern?**

- Art. 45 GDPR

**5.3. Explain why this has been an issue for your stakeholders?**

5.4. **What are differences that you have encountered between stakeholders in your Member State?**

5.5. **What are solutions to this issue? Please describe if these solutions are already implemented or potential, and whether this solution is provided by the SA or the stakeholders.**

## Part III – Actions by the SA

1. **Have you taken action (i.e. fact finding exercises, informal contact, prior consultation, investigation) towards any of the stakeholders concerning the use of cloud based services *prior to* launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

- Stakeholder has been advised to report follow-up assessments and measures taken.

2. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (e.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**

## Part IV – Other

1. **What is your general impression of the levels of awareness and compliance of the stakeholders you consulted concerning the use of cloud?**

- During the pre-contractual-phase awareness was actually quite high, seeing as numerous bodies (internal and external) were counsulted beforehand. Follow-up measures have been advised.

2. **Are there any other issues or topics that you would like to flag?**

3. **Are there any best practices that you would like to share?**

# BE SA

## (Autorité de protection des données – Gegevensbeschermingsautoriteit)

### Part I – Statistics

**4. How many stakeholders have you contacted within the following categories?**

- Ministry of the central government: The BE SA sent the questionnaire to 1 Ministry of the central government. This Ministry has the specificity of also being a member of the non-profit organisation (see below, under "other") that provides a community cloud. This set up has an impact on the answers provided by the Ministry.
- Independent public body of the central government: 1
- Buyer for the central government
- Publicly owned company acting as a processor for several central public bodies
- Ministry of the regional government: 5
- Independent public body of the regional government
- Buyer for the regional government
- Publicly owned company acting as a processor for several regional public bodies
- Other, please specify: **1 non-profit organisation (publicly owned) that acts as an independent internal ICT service provider for public bodies. This entity acts as a processor for the public bodies and also provides a community cloud.**

- In total, the BE SA sent the questionnaire to 8 stakeholders.

**5. How many stakeholders have you contacted within the following sectors?**

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government: **2**
- Economic affairs
- Education
- Finance
- Health: **1**
- Infrastructure
- Employment
- Justice
- Tax
- Other, please specify: **5 "regional" or "community" bodies that have competencies in the fields of health, education, etc.**

**6. If you have contacted a buyer, for which sectors does this buyer provides its services:**

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government
- Economic affairs
- Education
- Finance
- Health
- Infrastructure
- Employment
- Justice

- Tax
- No specific sector
- Other, please specify: **The BE contacted an independent internal ICT service provider for public bodies (the non-profit mentioned above) but the BE SA did not ask for which sector the latter provides its services as this question was not included in the original questionnaire, so the BE SA does not have this information.**

**7. <u>If you have contacted a buyer, and if you have this information, please specify the number of stakeholders this buyer provides services for:</u>**

- The BE SA remained faithful to the original questionnaire so does not have this information.

**8. <u>What was the initial procedural framework of your action?</u>**

- Fact finding
- Fact finding + determining follow-up action based on the results
- New investigation[1]
- Ongoing investigation

- The initial procedural framework of the action was a fact-finding mission. The objective was to obtain a helicopter view of the use of cloud-based services by public bodies. It was decided that the possible follow-up action(s) would be determined on the basis of the answers to the questionnaire.

**9. <u>How many stakeholders indicated that they use CSPs or are planning to do so in the near future (end of 2022)?</u>**

- 6 out of 8 stakeholders confirmed that they currently use CSPs.

**10. <u>Of the stakeholders that use CSPs (or are planning to do so in the near future), how many use CSPs for the following functions?</u>**

- Internal organisation (office suites, internal communication, HR, etc.)
- Exercise of public functions (services to citizens, processing citizen's data, etc.)

- The BE SA asked the respondents to answer the questionnaire only in relation to the most important CSPs used for large-scale processing of personal data of citizens. The BE SA decided not to focus its attention on the use of CSPs for internal organisation purposes, but only in relation to the public bodies' "core" functions/activities.

- Therefore, the BE SA cannot provide a response to this question, given that the BE SA does not have an overview of the use of CSPs for internal organisation purposes.

**11. <u>For the following commonly identified sectors, please specify if any hyper-scalers[2] are involved (if so please name them) either because they provide the services themselves or because the services are using the infrastructures of these hyper-scalers</u>**

- Health
- Finance
- Tax
- Education

[1] making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred

[2] Hyper-scalers provide cloud services at scale. It refers usually to the big cloud providers (Google, AWS, Microsoft …) on which other services may also depend

- Central buyers or providers of IT services

- The following hyper-scalers were mentioned in the questionnaires: AWS, Microsoft.

**12. <u>How many stakeholders took the following actions prior to- or during the acquisition of a CSP?</u>**

- *Perform a DPIA:* **2 out of 6 stakeholders.**
- *Does the DPIA analyse transfers in details (sometimes called DTIA):* **the BE SA does not have this information, as the DPIAs were not communicated by the stakeholders.**
- *Contact the DPO for advice:* **3 out of 6 stakeholders**.
- *Perform a general risk analysis:* **the BE SA does not have this information, as this specific question was not included in the questionnaire.**
- *Contact the SA for advice:* **this question was not included in the questionnaire but to our knowledge, the BE SA was not consulted by the stakeholders.**

**13. <u>How many stakeholders (including buyers) take the following actions during the use of the CSP?</u>**

- Monitoring technical and organisational measures to ensure compliance: **3 out of 6 stakeholders monitor technical and organisational measures.**
- In case of transfers, adopting technical and organisational measures, including supplementary measures, where needed, and monitoring if changes in the regulatory landscape occur (e.g. Schrems II): **<u>2 out of 6 stakeholders responded that transfers take place. If transfers take place, technical and organisational measures have been adopted by the stakeholders. Sometimes the technical and organisational measures were not specifically described by the stakeholders. 1 stakeholder (out of 2) claimed that it monitors changes in the regulatory landscape.**
- Regular risk assessments: **2 out of 6 stakeholders responded that they make regular data protection risk assessments. 1 out of 6 stakeholders responded that they make regular data protection risk assessments but without providing clear answers as to the process so the BE SA is not certain that such assessments take place in practice.**

## Part II – Substantive issues

**1. <u>The DPO was not consulted</u>**

- In some cases, the DPO was not consulted prior to selecting and acquiring the services of the CSP.

- However, article 39(1) of the GDPR clearly stipulates that:

- The data protection officer shall have at least the following tasks:

*"(a) to **inform and advise** the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;*

*(b) to **monitor compliance** with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;*

*(c) to **provide advice** where requested as regards the **data protection impact assessment** and monitor its performance pursuant to Article 35;*

(…)".

- One stakeholder did not consult its own DPO as it provides the community cloud and acts as a processor. This does not seem to be a valid argument as Article 37 of the GDPR applies to both controllers and processors with respect to the designation of a DPO and the tasks of the DPO listed on Article 39 of the GDPR applies to processor and controller DPOs.

- One stakeholder did not consult its own DPO, as it is a member of the said non-profit. However, this does not, in our opinion, constitute valid reasons not to consult the DPO in the context of the use of cloud services.

- In addition, one stakeholder did not consult its DPO because it acquired the cloud services through a central regional buyer. Again, this does not, in our opinion, constitute a valid motive not to involve the DPO of the controller.

- Three stakeholders consulted the DPO and sought an opinion. One of these stakeholders detailed that the DPO was involved at different stages of the acquisition of the cloud services, i.e. when preparing the tender documents and throughout the selection process.
- As indicated in the Guidelines on Data Protection Officers ('DPOs'), the GDPR recognises the DPO as a "key player in the new data governance system"[3].

- In some cases, it appears that the DPO has been side-lined entirely and is not granted this key position in important decisions that involve data protection issues.

**2. <u>Carrying out a DPIA</u>**

- A number of the stakeholders did not carry out a data protection impact assessment before selecting and using the services of the CSPs.

- The reasons provided for not carrying out a DPIA are not always based on legal arguments, for example, that the processing carried out in the context of the use of cloud services does not meet the conditions either listed in Article 35(3) of the GDPR or in the list established by the SA.

- One stakeholder did not carry out a DPIA as it does not act as a controller but supports the controllers it provides the community cloud to when they are carrying out a DPIA.

- One stakeholder considers that it must not carry out a DPIA due to the fact that it is a member of the non-profit providing the community cloud. This does not seem like a valid argument.

- One stakeholder confirms that various DPIAs have been performed, but it is not clear if the DPIAs also address the processing carried out in the context of the use of cloud services.

- One stakeholder affirms that it intends to use the DPIA carried out and made public by the Nederlandse Rijksoverheid entitled "Public DPIA Team OneDrive Sharepoint and Azure". The stakeholder intends to analyse the scope of the DPIA and shall make an additional DPIA concerning its use of CSPs if needed. The analysis is ongoing, despite the fact that the cloud services have been in use for some time. However, Article 35(1) of the GDPR clearly stipulates that a DPIA must be carried out prior to the processing. In addition, a DPIA must take account of the nature, scope, context and purposes of the specific processing envisaged. The stakeholder

[3] Guidelines on Data Protection Officers ('DPOs') of the Art. 29 Data Protection Working Party, p. 5.

must therefore carry out its own DPIA that relates specifically to the processing done by the CSP on its request.

- The DPIA, which constitutes an important tool for accountability, is a "*process for building and demonstrating compliance*"[4]. This does not seem to be understood by several of the stakeholders.

- Stakeholders must understand that the DPIA has to be carried out before the processing starts and also that they must carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations (article 35(11 of the GDPR).

**3. <u>Data protection requirements in the public procurement documents</u>**

- Article 28(1) of the GDPR stipulates that "*Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject*".

- Despite this obligation, several of the public bodies did not include detailed data protection requirements or certification requirements in the tender/public procurement documents. This seems to indicate that the obligation to "only use processors providing sufficient guarantees" is not fulfilled as data protection requirements are not taken into account when choosing the CSPs.

- In one case, the stakeholder argued that this was due to the fact that it went through a central regional buyer to acquire the CSP and so had no control over the tender process or the requirements included in the documents. The stakeholder argues it does not have the means to organise tenders.

- Another stakeholder, that benefited from a European framework agreement to use the cloud services, affirmed that information security requirements were included in the tender (including ISO 270001 certification).

- Yet another stakeholder included detailed requirements in relation to data protection in its tender documents: confidentiality, technical and organisation measures, restriction of transfers to third parties, rights of the data subjects, deletion or return of the data at the end of the contract, etc.).

- Including such requirements in the public procurement seems to be essential to ensure that only processors complying with data protection requirements and therefore meeting the conditions set out in Article 28 of the GDPR are selected by the controllers.

**4. <u>Contract between the controller and the CSP</u>**

- Two stakeholders had not yet signed a contract pursuant to Article 28(3) of the GDPR with the CSP, even though the processing is already ongoing.

- This is problematic as Article 28(3) of the GDPR clearly stipulates that the processing by the processor shall be governed by a contract or other legal act under Union or Member State law that is binding on the processor with regard to the controller.

[4] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 of the Art. 29 Data Protection Working Party, p.4.

- Some stakeholders indicated that the CSPs standard contract had to be concluded in order to use the services and there was no possibility to negotiate a bespoke contract. This may be problematic in relation to the content of the contract and its conformity with article 28(3) of the GDPR, leaving no margin of negotiation for the controller and therefore possibly not enabling the controller to remain in control of the personal data.

- The controllers should make sure that such contracts are signed before the start of the processing and that they contain all the requirements if Article 28(3) of the GDPR.

- The standard contracts signed by some of the stakeholders contained general authorisation to use sub-processors, as allowed by Article 28(2) of the GDPR: "*The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes*". The question of whether the controller is offered a meaningful opportunity to object to changes of sub-processors is raised.

**5. <u>International transfers</u>**

- In one case, the stakeholder seemed to provide contradictory information in relation to the possible transfers to third countries, which indicates that the controller does not always have a clear picture of the data transfers operated by the CSPs in the context of the execution of the contract.

- In another case, the stakeholder responded that transfers take place only to one country with an adequacy decision. However, in the standard contract of the CSP the stakeholder refers to, it is clearly stipulated that the data will be processed only in the locations specified by the customer, "*except as necessary to provide the Services initiated by the Customer or as necessary to comply with the law or binding order of a governmental body*".

- It appears that some stakeholders have limited knowledge of whether third country transfers take place.

- Several stakeholders did not check, in light of the Schrems II judgement, that there is nothing in the third country's legislation and/or practices that prohibits the recipients from complying with their contractual obligations in order to ensure that the level of data protection of natural persons guaranteed in the EEA is not undermined.

- The stakeholders should ensure that they have precise information on the actual transfers of personal data to third countries that take place and that the processors they select respect the provisions of Chapter V of the GDPR and the Schrems II ruling.

## Part III – Actions by the SA

**1. <u>Have you taken action (i.e. fact-finding exercises, informal contact, prior consultation, investigation) towards any of the stakeholders concerning the use of cloud-based services prior to launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the stakeholder, general guidance,</u>**

**corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

- No, the BE SA did not launch any action prior to launching the coordinated action.

2. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (E.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**

- The BE SA waited for the outcome of the discussions within the CEF in order not to compromise any of the work done within the working group. The BE intends to send letters to the stakeholders to which the questionnaires were sent. The objective is to enable the stakeholders to make a self-assessment and take the necessary measures to comply with their data protection obligations and possibly also renegotiate the terms with the CSPs.

## Part IV – Other

1. **What is your general impression of the levels of awareness and compliance of the stakeholders you consulted concerning the use of cloud?**

- The BE SA's general impression is that there are big disparities in the level of awareness and compliance of the stakeholders.

- 1 stakeholder had a very high level of compliance/awareness. 4 stakeholders had medium to high level of compliance and 1 stakeholder had very low levels of compliance/awareness.

- In some cases, this was partially explained by the fact that the stakeholder had acquired the CSP's services through a central buyer. Consequently, there was some misperception on the allocation of responsibilities (consulting its own DPO, carrying out a DPIA, etc.) but also little to no control over the public procurement process.

2. **Are there any other issues or topics that you would like to flag?**

- No.

3. **Are there any leading practices of the stakeholders you have contacted that you would like to share?**

- No.

# CY SA

## Office of the Commissioner for Personal Data Protection (Cyprus SA)

### Part I – Statistics

1. **How many stakeholders have you contacted within the following categories?**

- We have contacted the Deputy Ministry of Research, Innovation and Digital Policy (DMRIDP), which acts as the buyer for the central government as regards to cloud services.

2. **How many stakeholders have you contacted within the following sectors?**

- Digitalisation of the Public Administration/e-Government (DMRIDP as mentioned above)

3. **If you have contacted a buyer, for which sectors does this buyer provides its services:**

- Digitalisation of the Public Administration/e-Government

4. If you have contacted a buyer, and if you have this information, please specify the number of **stakeholders this buyer provides services for:**

- All public bodies under the Central Government.

5. **What was the initial procedural framework of your action?**

- Fact finding + determining follow-up action based on the results

6. How many stakeholders indicated that they use CSPs or are planning to do so in the near future **(end of 2022)?**

- 1 (DMRIDP)

7. **Of the stakeholders that use CSPs (or are planning to do so in the near future), how many use CSPs for the following functions?**

- Internal organisation (office suites, internal communication, HR, etc.)

8. **For the following commonly identified sectors, please specify if any hyper-scalers[5] are involved (if so please name them) either because they provide the services themselves or because the services are using the infrastructures of these hyper-scalers**

- Central buyers or providers of IT services (Microsoft)

9. **How many stakeholders took the following actions prior to- or during the acquisition of a CSP?**

- Perform a DPIA: **1 DMRDP**
- Does the DPIA analyse transfers in details (sometimes called DTIA): **1 (DMRIDP) (although not in detail)**
- Contact the DPO for advice
- Perform a general risk analysis: **1 (DMRIDP)**
- Contact the SA for advice: **1 (DMRIDP)**

10. **How many stakeholders (including buyers) take the following actions during the use of the CSP?**

- Monitoring technical and organisational measures to ensure compliance: **1 (DMRIDP)**

[5] Hyper-scalers provide cloud services at scale. It refers usually to the big cloud providers (Google, AWS, Microsoft …) on which other services may also depend

- In case of transfers, adopting technical and organisational measures, including supplementary measures, where needed, and monitoring if changes in the regulatory landscape occur (e.g. Schrems II): **1 (DMRIDP)**
- Regular risk assessments: **1 (DMRIDP)**

## Part II – Substantive issues

- The DMRIDP, as mentioned on their answers from the questionnaire, has already proceeded with the purchase of 1500 licences of Microsoft Office 365 and is planning to sign an Enterprise Agreement for online cloud products such as Microsoft Teams, OneDrive and SharePoint. Moreover, after studying the DPIA and further responses to our questions, our SA has identified the following issues connected with this purchase

**1. Issue 1**

- The DMRIDP cannot guarantee that the use of the Microsoft's cloud service is compliant with the Schrems II ruling. There is a high data protection risk related to the possible access by US law enforcement and national security services to personal data and special categories of personal data. This risk occurs even though Microsoft Teams, OneDrive and SharePoint content data are exclusively processed and stored in the EU. Access to data on the EU located servers can be also ordered through US legislation such as the US CLOUD Act.

- As mentioned in the DPIA, this high risk can be mitigated for OneDrive and SharePoint by using their own encryption keys, with Microsoft Double Key Encryption. Microsoft does not yet offer end- to-end encryption for the streaming communication with multiple participants in Teams, only for unscheduled one-to-one video calls. Though Microsoft has confirmed that it will support E2EE in Teams group meetings and chat, it does not yet provide a deadline.

- For non-sensitive categories of personal data, the transfer risks are assessed as very low according to the DPIA, even though the possible impact on data subjects can be very high. The chance that Microsoft is compelled to disclose personal data from EU public sector customers is very slim. Though Microsoft cannot disclose if it has received any specific legal demands subject to a secrecy obligation. Microsoft publicly explains: "Microsoft does not provide, and has never provided, EU public sector customer's personal data to any government." This historical fact, combined with the use of the encryption applied by Microsoft, its legal guarantees of contesting each order, its proven track record and its transparency reports, may be sufficient to qualify the risk of undue access to the 'regular' personal data as a low data protection risk.

**2. Issue 2:**

- Microsoft shares data with third parties acting as sub-processors to support functions such as customer and technical support, service maintenance, and other operations. In such cases, there is a risk of losing the control of the relevant data. Additionally, it is difficult to monitor the level of protection applied by the sub-processors, thus the DMRID as the controller, will not be able to prove compliance with Articles 24 and 28 GDPR.

- In the DPIA it is mentioned that any subcontractors to which Microsoft transfers Support and Consulting Data will have entered into written agreements with Microsoft that are no less protective than the data protection terms of the MPSDPA. All third-party sub-processors with which Support and Consulting Data Is shared under the MPSDPA are included in the Microsoft Commercial Support Contractors List.

- Microsoft will not disclose Support and Consulting Data to US authorities unless required by law. If US authorities contact Microsoft with a demand for Support and Consulting Data, Microsoft will attempt to redirect the law enforcement agency to request the data directly from the customer. If compelled to disclose Support and Consulting Data to law enforcement, Microsoft will promptly notify the customer and provide a copy of the demand unless legally prohibited from doing so.

- Upon receipt of any other third-party request for Support and Consulting Data, Microsoft will promptly notify the customer unless prohibited by law. Microsoft will reject the request unless required by law to comply. If the request is valid, Microsoft will attempt to redirect the third party to request the data directly from the customer.

3. **Issue 3:**

- Transfer of telemetry/diagnostic data to the US. Diagnostic data is used to keep Office secure and up-to-date, detect, diagnose and remediate problems, and also make product improvements.

- According to Microsoft, this data does not include a user's name or email address, the content of the user's files, or information about apps unrelated to Office. This diagnostic data is collected and sent to Microsoft about Office client software running on the user's device in the client organization.

- There are three levels of diagnostic data for Microsoft 365 Apps for enterprise client software:
    - Required: The minimum data necessary to help keep Office secure, up-to-date, and performing as expected on the device it is installed on.
    - Optional: Additional data that helps to make product improvements and provides enhanced information to help detect, diagnose, and remediate issues.
    - Neither: No diagnostic data about Office client software running on the user's device is collected and sent to Microsoft. However, it is not clear whether this option differentiates from the above option “Required” as regards to the data collected.

- Microsoft has not provided an exact description of what data is collected and sent to the US for diagnostic purposes. Additionally, there does not seem to be a way to turn off Office telemetry completely.

- The DRMID, through their own investigation found that, though Microsoft will still transfer some personal data to the USA, to detect and solve security incidents, these ongoing transfers will be incidental, not structural, and they will generally only involve pseudonymised and aggregated data, thus minimizing the risks involved.

## Part III – Actions by the SA

1. **Have you taken action (i.e. fact-finding exercises, informal contact, prior consultation, investigation) towards any of the stakeholders concerning the use of cloud-based services *prior to* launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

- The DMRID has shared with our SA the strategy regarding the general use of cloud services by the central government, specifically the development of a hybrid private government cloud for use

by all public authorities. Following this, and a proposed DPIA received regarding the registration of elementary student using a cloud storage service, the Commissioner deemed it necessary, in carrying out her duties under the General Data Protection Regulation (EU) 2016/679, in compliance with the provisions of Article 57(1) (c), to inform the DMRIDP fully about all aspects and parameters relating to the provision of cloud computing services and in particular with regard to the risks that these services may entail. It was also pointed out that in the case of public authorities, which collect and process citizens' personal data on the basis of their legal obligations or in the exercise of the public authority granted to them, citizens, as data subjects, do not have reasonable expectation that their data collected by a public authority is transmitted and hosted in data centres of the provider or its partners in various third countries. This rationale makes even greater the obligation of the public authorities to take every possible action for ensuring the proper transparency of the process, by properly informing the data subjects, in compliance with the provisions of Articles 13 and 14 as the case may be.

2. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (E.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**

- Currently, our SA plans to continue issuing recommendations to the DMRIDP and ensure that no CSPs are obtained without taking the appropriate remedies for the risks identified. Moreover, in the case of non-compliance or cooperation by the DMRIDP or any public body using CSPs, the Commissioner will also consider using corrective measures if necessary. Our SA will also take into consideration the results of the coordinated action as well as any developments regarding the new USA adequacy decision under discussion.

## Part IV – Other

1. **What is your general impression of the levels of awareness and compliance of the stakeholders you consulted concerning the use of cloud?**

- Overall, we believe that the DMRIDP was fully aware of the risks involved when purchased the licenses for the use of Microsoft 365 tools (Teams, OneDrive, and SharePoint). While we acknowledge that the integration of such tools is important for the digitalization of services offered to the public, we remain concerned, that in the absence of an adequacy decision, the transfer of data to the US and/or third countries' subcontractors and/or the US Authorities potential access to data stored in the EU, relies on standard contractual clauses, for which third parties such as the DMRIDP have little or no power of control.

2. **Are there any other issues or topics that you would like to flag?**

3. **Are there any leading practices of the stakeholders you have contacted that you would like to share?**

# CZ SA

## Úřad pro ochranu osobních údajů – The Office for Personal Data Protection

**In needs to be stated, that the onsite inspection is still ongoing to the date of submission of this National Report. All the preliminary findings stated bellow are still subject to the examination.**

### Part I – Statistics

1. **How many stakeholders have you contacted within the following categories?**

- Ministry of the central government: **2**
- Independent public body of the central government: **1 (NOTE: The National Agency for Communication and Information Technologies is a state-owned company established in accordance with Act No. 77/1997 Coll., On State Enterprises, the founder is the Ministry of the Interior. It is a legal entity carrying out business activities with state property in its own name and under its own responsibility. However, it is not independent public body of the central government.)**

2. **How many stakeholders have you contacted within the following sectors?**

- Digitalisation of the Public Administration/e-Government: **1 – National Agency for Communication and Information Technologies (NAKIT)**
- Economic affairs
- Education
- Finance
- Health
- Infrastructure
- Employment: **1 – Ministry of Labour and Social Affairs (MoLSA)**
- Justice
- Tax
- Other, please specify: **Internal affairs: 1 – Ministry of Interior (MoI)**

3. **If you have contacted a buyer, for which sectors does this buyer provides its services:**

- Not applicable

4. **If you have contacted a buyer, and if you have this information, please specify the number of stakeholders this buyer provides services for:**

- Not applicable

5. **What was the initial procedural framework of your action?**

- Fact finding + determining follow-up action based on the results

6. **How many stakeholders indicated that they use CSPs or are planning to do so in the near future (end of 2022)?**

- All stakeholders currently use CSPs.
- Two stakeholders (NAKIT and MoI) identified one (the same) cloud-based service that processes personal data, The Citizen's Portal. MoI is the controller while NAKIT is the processor. Neither NAKIT nor MoI indicated any use of CSPs in another instance. (NOTE: The answers to all of the following questions apply only to NAKIT and MoI and all of the answers apply to The Citizen's Portal. Since the CSP is used to run The Citizen's Portal, all the answers are given on behalf of MoI as the controller while NAKIT as the processor is regarded as NOT using CSP at all)

- One stakeholder (MoLSA) claims not to use them for such processing. 1 stakeholder (NAKIT) claims not to use CSPs at all (other then CSP used to run the Citizen's Portal).

7. **Of the stakeholders that use CSPs (or are planning to do so in the near future), how many use CSPs for the following functions?**

– Internal organisation (office suites, internal communication, HR, etc.)
– Exercise of public functions (services to citizens, processing citizen's data, etc.): **1**

8. **For the following commonly identified sectors, please specify if any hyperscalers are involved (if so please name them) either because they provide the services themselves or because the services are using the infrastructures of these hyper-scalers**

– Central buyers or providers of IT services: **1 stakeholder utilizes Microsoft Azure.**

9. **How many stakeholders took the following actions prior to- or during the acquisition of a CSP?**

– Perform a DPIA: **1**
– Does the DPIA analyse transfers in details (sometimes called DTIA): **No**
– Contact the DPO for advice: **1**
– Perform a general risk analysis: **1**
– Contact the SA for advice: **0**

10. **How many stakeholders (including buyers) take the following actions during the use of the CSP?**

– Monitoring technical and organisational measures to ensure compliance: **1**
– In case of transfers, adopting technical and organisational measures, including supplementary measures, where needed, and monitoring if changes in the regulatory landscape occur (e.g. Schrems II): **Data centres are in the EU, no transfer takes place.**
– Regular risk assessments: **1**

## Part II – Substantive issues

1. **DPIA**

- Preliminary findings suggest that the DPIA has not been thoroughly done accordingly to the items set out in Art. 35(7) GDPR. MoI is of the opinion that a DPIA is not a mandatory document in this case.
- Art. 35 GDPR, Article 10 of Act No. 110/2019 Coll., On Personal Data Processing.
- Preliminary findings suggest that the DPIA does not reflect whether alternatives (other than a cloud-based service) were considered. Moreover, the DPIA does not contain any assessments as required by Art. 35(7) (b/c) GDPR.
- Requirements laid down in Art. 35(7) (d) GDPR appear not to be met – the DPIA lists the measures taken, but they are not assigned to the risks. It is not clear, what specific measures were taken to mitigate a particular risk.
- Preliminary findings have revealed that the DPO of the controller was not involved in the manner prescribed by Art. 35(2) GDPR.
- Furthermore, the controller is of the opinion that any DPIA is not needed at all pursuant to Article 10 of Act No. 110/2019 Coll., On Personal Data Processing. This section of the national law states that a controller is not obliged to carry out DPIA in the situation where it is stated by law that the controller has to carry out a specific processing operation. The CZ SA has opposed to such interpretation of the national law, as it was not interpreted in accordance with the GDPR.
- Not applicable

- If the preliminary findings are upheld, the CZ SA will insist that the controller takes measures to amend the DPIA. The controller will be approached due to the differing opinions on whether the DPIA is obligatory.

**2. Contract pursuant to Art. 28 GDPR**

- Preliminary findings suggest that only a general contract between the controller (MoI) and the processor (NAKIT) has been concluded.
- Art. 28 GDPR, mainly Art. 28 (3) GDPR.
- Preliminary findings indicate, that there is only a general contract between the controller (MoI) and the processor (NAKIT) (it needs to be noted that there are two more sub-processors, T-Mobile Czech Republic a.s. and MICROSOFT s.r.o. at the end) that serves as a basis for a range of services provided by the processor to the controller, whereas only one of them is The Citizen's Portal. This appears to constitute a breach of Art. 28 (3) GDPR that stipulates, that a contract shall set out "the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects", since none of the cited is specified in the contract in relation to The Citizen's Portal.
- Not applicable
- The controller will be obliged (in case the above stated findings have been confirmed) by the CZ SA to amend the contract so it is specific as per requirements set out in Art. 28 (3) GDPR.

**3. Use of Microsoft Azure**

- The MoI declared the use of Microsoft Azure as their cloud platform.
- Articles 44-49 GDPR may be concerned.
- In light of the Schrems II judgment, it is not clear whether the use of such services involves the transfer of personal data (e.g. IP addresses) to the United States of America.
- Not applicable
- According to the MoI, contracts with providers were set up so that all data processed under the use of cloud services were stored exclusively in data centres geographically located in the EU. Further investigation will show whether this condition has been met. It will also be necessary to decide whether such conditions are sufficient in the light of Schrems II.

## Part III – Actions by the SA

**1. Have you taken action (i.e. fact-finding exercises, informal contact, prior consultation, investigation) towards any of the stakeholders concerning the use of cloud-based services *prior to* launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

- Only a general communication on principles regarding transfers of personal data to 3rd countries took place.

**2. What action(s) are you planning to undertake based on the results of this coordinated action, if any? (E.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**

- An on-site inspection is currently under way. Based on the facts established, consideration will then be given to the possible further use of the investigative and corrective powers vested in the CZ SA.

## Part IV – Other

1. **What is your general impression of the levels of awareness and compliance of the stakeholders you consulted concerning the use of cloud?**

- It can be stated that a potentially problematic issue of personal data transfer to 3rd countries has been identified, however, it is clear from the stakeholder's statements that they are at least aware of these risks and try to mitigate them in certain ways, such as using data centres in the EU. Furthermore, it is the impression of the CZ SA that while focus (rightfully so) of the controller is given to the obligations under Art. 25 and 32, other obligations under the GDPR are neglected, mainly those related to Art. 28 and 35 GDPR.

2. **Are there any other issues or topics that you would like to flag?**

- Not applicable

3. **Are there any leading practices of the stakeholders you have contacted that you would like to share?**

- Not applicable

# DE SA

## Part I – Statistics

1. **How many stakeholders have you contacted within the following categories?**

- Ministry of the central government
- Independent public body of the central government
- Buyer for the central government
- Publicly-owned company acting as a processor for several central public bodies: **1**
- Ministry of the regional government: **1**
- Independent public body of the regional government
- Buyer for the regional government
- Publicly-owned company acting as a processor for several regional public bodies
- Other, please specify: **8 (categories: health insurance, processor for health insurance, pension insurance, labour administration, central it service provider)**

2. **How many stakeholders have you contacted within the following sectors?**

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government: **2**
- Economic affairs
- Education
- Finance
- Health: **6**
- Infrastructure
- Employment: **1**
- Justice
- Tax
- Other, please specify: **1 pension insurance**

3. **If you have contacted a buyer, for which sectors does this buyer provides its services:**

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government
- Economic affairs
- Education
- Finance
- Health
- Infrastructure
- Employment
- Justice
- Tax
- No specific sector: **2**
- Other, please specify: **IT service provider for the federal public sector**

4. **If you have contacted a buyer, and if you have this information, please specify the number of stakeholders this buyer provides services for:**

- Information not provided.

5. **What was the initial procedural framework of your action?**

- Fact finding: **X**
- Fact finding + determining follow-up action based on the results
- New investigation
- Ongoing investigation

6. **How many stakeholders indicated that they use CSPs or are planning to do so in the near future (end of 2022)?**

- 9

7. **Of the stakeholders that use CSPs (or are planning to do so in the near future), how many use CSPs for the following functions?**

- Internal organisation (office suites, internal communication, HR, etc.): **8**
- Exercise of public functions (services to citizens, processing citizen's data, etc.): **up to 4**

8. **For the following commonly identified sectors, please specify if any hyper-scalers are involved (if so please name them) either because they provide the services themselves or because the services are using the infrastructures of these hyper-scalers**

- Health: **5**
- Finance
- Tax
- Education
- Central buyers or providers of IT services: **3**
- pension insurance: **1**

9. **How many stakeholders took the following actions prior to- or during the acquisition of a CSP?**

- Perform a DPIA: **3**
- Does the DPIA analyse transfers in details (sometimes called DTIA): **2**
- Contact the DPO for advice: **3**
- Perform a general risk analysis: **6**
- Contact the SA for advice: **1**

10. **How many stakeholders (including buyers) take the following actions during the use of the CSP?**

- Monitoring technical and organisational measures to ensure compliance:
- In case of transfers, adopting technical and organisational measures, including supplementary measures, where needed, and monitoring if changes in the regulatory landscape occur (e.g. Schrems II): **4**
- Regular risk assessments: **7**

## Part II – Substantive Issues

**Preliminary note**

The DE SAs investigated a total of 10 public entities at federal and regional level. As the individual projects examined differ greatly from one another the following report is divided in parts and sections. Each part/section is dedicated to one or more DE public institutions. The first part deals with stakeholders actually using cloud service, while the second part examines a proof of concept concerning the use of an intermediate encryption service.

**Part II.1. Stakeholders actually using cloud services**

General remarks on the subject of questions I., 2. g) -j) (personal data):

A) 1. In the case of identical task areas, an allocation of data processing processes, in particular to the higher level of protection according to Art. 9 GDPR (above all health data) by the supervised bodies is inconsistent.

Applications from CSPs are used by public bodies for identical areas of responsibility. The statements of the supervised bodies differ as to whether the data processing concerns core areas of the fulfilment of tasks and whether this at least also involves health data, which are subject to the higher level of protection under Art. 9 GDPR.

2. Relevant regulations:
a. Art. 5 GDPR
b. Art. 6 GDPR
c. Art. 9 GDPR
d. Art. 4 GDPR
e. Art. 28 GDPR
f. Art. 32 GDPR
g. sec. 35 para. 2 of the German Social Code (SGB) Book I, sec. 67 ff. of the German Social Code Book X

The questions mentioned under point 1 have a direct effect on the assessment of the lawfulness of the data processing - especially in the area of Art. 9 GDPR. The question of whether health data are processed by the CSP determines the opening of the scope of protection of Art. 9 GDPR. The question of whether health data are processed for the core area of task fulfilment primarily leads to legal reviews under Art. 32(2) of the GDPR and Section 80(2) of the German Social Code Book X. If health data are processed by the CSP outside the core area of task fulfilment, it must be examined whether the legal grounds for permission apply or whether explicit consent is required according to Art. 9 para. 2 lit. a) GDPR. In the latter case, in addition to the challenge of an informed decision, the aspect of "voluntariness" is also problematic due to the subordination relationship.

Due to the broad variance in descriptions, the data processing by the CSP could also first be reviewed on the basis of the data minimisation principle.

The common interest is to be able to guarantee the fulfilment of tasks and to have legally compliant and suitable data processing means available on the market for this purpose and to be able to use them in a data protection compliant manner. First, a uniform terminological understanding of data protection must be created and the corresponding data processing procedures must be reflected transparently.

B) Regarding one central IT service provider no substantial issues have been identified from the information provided. However, the report did not seem to be complete and an improved version has not been delivered in time, although a revised document was requested.

The only productive cloud service described is cloud hosted by the service provider itself, providing various IaaS, PaaS, and SaaS services for public authorities.

The supervisory authorities have been involved as consultant from an early phase. The service provider only acts as processor, controllers are assisted with DPIOs, if necessary. As no actions were planned, contracts have not been requested with the questionnaire therefore no assessment can be made.

The self-hosted cloud is only operated in the service provider’s data centres located in Germany and services are only provided to German public bodies. No data transfers to third countries occur.
Diagnostic data is collected according to the BSI Act, which provides the legal basis for possible measures in this field

Implementation of technical and organizational matters as well as compliance with the data protection concept is ensured via regular audits by the supervisory authority.

C.) 1. Personal data (communication data) is collected via registration and in the context of participation in the virtual event. Special categories of personal data or social data are not processed. An increased need for protection is not apparent. The transmission of telemetry data is prevented as far as possible. The processing of additional telemetry data generated in the cloud cannot be ruled out according to current knowledge.

2. Relevant regulations:
a. Art. 5 GDPR
b. Art. 6 GDPR
c. Art. 9 GDPR
d. Art. 4 GDPR
e. Art. 28 GDPR
f. Art. 32 GDPR
g. Sec. 26 of the German Federal Data Protection Act (BDSG)

The questions mentioned under point 1 have a direct effect on the assessment of the lawfulness of the data processing. The question of whether social data is processed for the core area of task fulfilment does not arise here after the feedback, so that a legal review according to Art. 32 para. 2 GDPR and sec. 80 para. 2 of the German Social Code (SGB) Book X is dispensable. Since employee data may also be affected here, the question of effective consent to data processing appears questionable. In addition to the challenge of an informed decision, the aspect of "voluntariness" is also problematic due to the subordination relationship.

The common interest is to be able to guarantee the fulfilment of tasks and to have legally compliant and suitable data processing means available on the market for this purpose and to be able to use them in a data protection compliant manner. First, a uniform terminological understanding of data protection must be created and the corresponding data processing procedures must be reflected transparently.

Thematic sensitisation can take place by means of information campaigns or on the occasion of supervisory measures.

**Part II.2. Substantive issues**

**Part II.2.1 Pre-Contract/Procurement Criteria**
- On the topic of "acquisition of cloud services”
1. Relevance and coverage of the data protection challenges/requirements for tenders and award decisions.

All surveys showed that data protection requirements are included in tendering and award procedures. The feedback, however, showed a variance in terms of bindingness or as possible grounds for exclusion. This can subsequently lead to problems, as procurement criteria cannot easily be changed after the award decision.

In some cases, pre-DPIAs, here essentially an analysis of the nine criteria for high-risk processing operations according to WP 248 of the Article 29 data protection working party, were conducted before the procurement to determine necessary data protection requirements.

2. Relevant regulations:
a. GDPR as a whole
b. Chapter 2 of the German Social Code (SGB) Book X
c. European and German public procurement law

3. The public bodies have to fulfil their legal duties. Due to digitisation strategies and economic considerations, processes must be redesigned, for which the market provides limited products. The mandatory data protection requirements are often in conflict with the technical requirements resulting from the legal mandates due to market conditions.

4. In some cases, stakeholders have joined forces in order to achieve a better negotiating position for the enforcement of data protection requirements. However, this approach could not completely eliminate the tension.

5. Data protection requirements must be brought to the attention of the market through supervisory measures but also through socio-political discussions. Furthermore, a joint approach of dealing with the existing discrepancies between the available products and the legal requirements/developments of data protection at the European level would be most welcome (especially against the background of the Schrems II decision of the ECJ).
In the future, "GDPR certifications" could be used as a suitable means for award criteria in IT tendering.

**Part II.2.2 International transfer**
On the subject of "Contract and International Transfer
A) 1. The problem is largely reflected in the widespread use of American applications. There is a transfer of data to third countries. This allows access for foreign governments even in the case of non-EU customer service providers who only offer their services from the EEA. The powers of the US intelligence services are problematic here; due to the legal situation in the USA, an adequate governmental level of data protection (Art. 45 DS-GVO) cannot be ensured. The standard contractual clauses adopted by the Commission in 2010 are no longer sufficient for data transfers to third countries without any additional measures.

2. Relevant regulations:
a. Art. 5 GDPR
b. Art. 6 GDPR
c. Art. 4 GDPR
d. Art. 28 GDPR
e. Art. 32 GDPR
f. sec. 80 para. 3 of the German Social Code (SGB), Book X in conjunction with Art. 45 GDPR
g. Art. 46 para. 1 GDPR

3. The stakeholder group is the health sector. All public bodies in the health sector that transfer data to the USA, especially if they have previously based the transfer on the Privacy Shield, but also if they used the old standard contractual clauses from 2010 for this purpose, transfer sensitive social and health data to third countries.
It is questionable whether the legitimate interests are safeguarded if a transfer is not made or the consent of the data subject is obtained. In principle, the general interest prevails.

4. Differences in stakeholder groups: There are hardly any transfers to third countries.
- Awareness of third country issues (Schrems II),
- Willingness to introduce further measures exists
- Implementation and further development of technical and organisational measures

5. Action will be taken with all stakeholders and awareness of third country issues will be raised. Contractual and technical restriction of processing to the EU will take place. In addition, further technical measures have been agreed to prevent personal data from leaving the geolocation (Premium Support Contract: Customer Lock Box, Local Support Engineer). Transfers of personal data outside the EU will have to be approved by the client on a case-by-case basis (e.g. for support).

In addition, the processing of personal data is regularly restricted to the EEA in the contracts with CSPs. Special attention will be paid to conclude contracts for the provision of cloud services generally only with CSPs located in the EEA. If, in individual cases, a CSP outside the EEA is appointed, contractual parties shall agree on further safeguards (e.g. in accordance with the requirements of the German and European data protection authorities) in addition to the inclusion of currently valid standard contractual clauses.

Encryption of data according to the "Bring your Own Key" principle and specific additional agreements for social data are planned.
The creation of security concepts is planned.
Further problems exist in the implementation of physical controls in the technical facilities of the third countries ("access controls").

B) 1. The issue is largely reflected in the use of a cloud offering from a third-country provider. Data transfer to third countries cannot be ruled out. This allows access for foreign governments even in the case of the use of non-EU account managers who only offer their services from the EEA. The powers of the US intelligence services are problematic here; due to the legal situation in the USA, an adequate state level of data protection (Art. 45 DS-GVO) cannot be ensured. The standard contractual clauses adopted by the Commission in 2010 are no longer sufficient for data transfers to third countries without additional measures. However, the current, adapted standard contractual clauses are used here.

2. Relevant regulations:
a. Art. 5 GDPR
b. Art. 6 GDPR
c. Art. 4 GDPR
d. Art. 28 GDPR
e. Art. 32 GDPR
f. sec. 80 para. 3 of the German Social Code (SGB), Book X with Art. 45 GDPR
g. Art. 46 para. 1 GDPR

3. The stakeholder group here is the education sector in the social administration department. It is questionable whether the legitimate interests would be safeguarded if the data were not transferred or if the consent of the data subject were obtained. In principle, the general interest prevails.

4. Differences in the stakeholder groups: Based on the questionnaires, it is clear that hardly any or no transfers take place to third countries. It can be concluded that there is
- Awareness of the third country problem (Schrems II)
- Willingness to introduce further measures - Implementation and further development of technical and organisational measures
- Implementation and further development of technical and organisational measures

5. Measures are being worked on with all stakeholders and awareness of the third-country problem is being raised. The current, adapted standard contractual clauses are used. The validity of German law, the use of European servers and the compliance with contractually agreed technical and organisational measures have been contractually agreed. Further problems exist in the implementation of physical

controls in the technical facilities of the third countries ("access controls"). The possibility of on-site inspections by the contracting authority and the competent legal and technical supervision was contractually agreed.

**Part II.2.3 Necessary telemetry data**

On the topic of "diagnostic/telemetry data":

1. Product-specific statements regarding the collection on user computers vs. CSP servers or the use of anonymised, pseudonymised or real data can only be made in general terms. Some diagnostic/telemetry data is considered to be non-personal data, although direct or indirect identification of data subjects cannot be excluded.

2. Relevant regulations:

a. Art. 5 GDPR
b. Art. 6 GDPR
c. Art. 4 GDPR
d. Art. 28 GDPR
e. Art. 32 GDPR

3. to 5. Primarily a technical referral is required to analyse the circumstances, assess interests and develop solutions.

**Part II.2.4 Monitoring/Compliance**

On the subject of "Contract and International Transfer

A) 1. The problem lies primarily in the unclear jurisdiction.

The implementation of long-term measures requires a precise definition of these additional measures, which must also be implemented in the next step, i.e. they must also be available effectively and practically. For some health insurance funds, the details for future audits have not yet been determined.

2. Relevant regulations:

a. Art. 5 GDPR
b. Art. 6 GDPR
c. Art. 4 GDPR
d. Art. 28 GDPR
e. Art. 32 GDPR
f. sec. 80 para. 3 of the German Social Code (SGB), Book X with Art. 45 GDPR
g. Art. 46 para. 1 GDPR

3. Implementation of procedures for dealing with data breaches and notifications pursuant to Articles 33 and 34 GDPR.

- Procedures for dealing with the exercise of the rights of the data subject.

This in turn may require further external monitoring for the health insurance funds. This external accompaniment could constitute a subcontracted processor.

4. Some health insurance funds are already carrying out risk assessments, whereas other health insurance funds must implement measures before doing so.

Details of the audits have not yet been determined; some software producer offer, among other things, that audits will be made (external audit also conceivable);

5. Among other things, group-wide data protection management systems (DSMS) and information management systems (ISMS) have been established at the statutory health insurance funds to ensure compliance with data protection laws and the security of the processing of personal data. Various

group-wide binding guidelines are derived from guidelines on data privacy and information security. Further solutions provide for existing risk analyses and DPIAs are to be reviewed every 2 years at the latest and that monitoring is to be carried out on the basis of the processor contract.
Risk assessments are carried out as part of the preparation and updating of the data protection impact assessment. In accordance with the Supplier Management Policy and "DSM Risk Assessment and the data protection impact assessment", the risk assessment is considered again in the regular service provider review as well as in the regular review of the documents and, if necessary, there is response to new finding.

B. 1. The control of technical and organisational measures is carried out by the responsible department through IT administration, IT security and the data protection unit. In addition, there is a regular exchange and further training. Monitoring of telemetry data is carried out by IT security and system administration in day-to-day business. However, monitoring is geared towards external attacks and irregularities. A procedural notification is available; a data protection impact assessment is still pending and is currently being prepared.)

2. Relevant regulations:
a. Art. 5 GDPR
b. Art. 6 GDPR 8
c. Art. 4 GDPR
d. Art. 28 GDPR
e. Art. 32 GDPR

C. One of the responses indicates that monitoring of security measures and information security risk assessments (ex-post) are only carried out if necessary, i.e., only contract adjustments and innovations on the part of the processor are reviewed. And further *"work is underway to establish a process"*.

**Part II.3. Investigation of a Proof of Concept (POC)**
Object of one investigation was a proof of concept (PoC). The stakeholder can be seen as central buyer in the sense of the CEF providing the contractual setting for different areas government / administration.
The concept of the PoC aims at encrypting data before it is transferred to the cloud by an intermediate encryption component. Background of the PoC is an announcement by a CSP to offer its products cloud based only in the near future. According to the stakeholder, the reason for conducting the PoC was therefore primarily to comply with data protection regulations, especially with a view to Articles 9, 28, 32, 44 et seqq. GDPR and corresponding national law.
To date, the PoC has not been implemented in a productive system. No contract had been negotiated and no personal data has been transported to a cloud. This has to be kept in mind when analysing the following.

1. Pre-contractual phase
The stakeholder seems aware of GDPR requirements (e.g. DPIA, technical and organisational measures, involving the DPO). The whole concept aims at ensuring the highest level of data protection when using cloud services. According to the stakeholder, only IP addresses would be transported to the cloud but no other data would be made accessible for the CSP.
However, the stakeholder states that data protection is only one argument when choosing a CSP. Functionality and convenience for government tasks are at least as important.

2. Contract with the CSP
The stakeholder assures that in any case it would secure the government's dispositional sovereignty over the processed data. To this end, before awarding a contract, it would be necessary the CSP accepts the terms set out in a model contract, which had been approved by the competent SA. This would

secure the requirements of Art. 28 GDPR. According to the stakeholder, this is also true with regard to Art. 28(3) (d) GDPR.
The stakeholder informs that there is a model contract negotiated with participation of the federal government and one of the major German digital associations. SCC would be used, according to the respective data being processed.

3. International transfers
The stakeholder emphasises, if the concept were implemented, there would be different legal requirements depending on the type of data being processed and the location of the cloud servers. A case-by-case approach would be conducted. The stakeholder would always analyse where the data is being transferred to, what legislations would be applicable insofar and which access options there would be (although, according to the concept, the data transfer should in principle be limited to IP addresses).

## Part III - Actions by the SA

1. **Have you taken action (i.e. fact-finding exercises, informal contact, prior consultation, investigation) towards any of the stakeholders concerning the use of cloud-based services prior to launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

- No

2. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (E.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**

- Discussions or awareness raising should take place on the occasion of supervisory measures. Measures will only be taken after leads have been agreed on how to deal with the issue of third-country transfers and thus a reliable framework for supervisory action is established.

## Part IV - Other

1. **What is your general impression of the levels of awareness and compliance of the stakeholders you consulted concerning the use of cloud?**

- They are all aware but cannot see a reliable framework to base their actions on? Shutting down CSP applications is de facto not an option.
- Regarding international data transfer it is stated, that no data transfers to third countries take place because only data centres located in Europe are used. There seems to be little awareness that, at the moment, using US-based cloud services is not usually possible without data transfer to the USA.
- Standards, contracts and non-GDPR certifications are taken as a basis to choose a cloud provider. A detailed review of the actual processing does not always take place.

2. **Are there any other issues or topics that you would like to flag?**

3. **Are there any leading practices of the stakeholders you have contacted that you would like to share?**

# EDPS

## European Data Protection Supervisor

**INTRODUCTION**

1. This report has been prepared in the context of the EDPB 2022 Coordinated Enforcement Action, which focuses on the use of cloud-based services by the public sector. One of its goals is to explore the challenges that public bodies face in terms of compliance with the GDPR[6]/EUDPR[7]. This includes the procedures for procuring cloud-based services and associated safeguards that must be implemented as well as the contractual and actual compliance with data protection rules, and in particular transfers outside the European Economic Area ('EEA') in view of the Schrems II judgment.[8]

2. The CEF further aims at fostering best practices by supervisory authorities through coordinated guidance and action, thereby ensuring the protection of personal data.

3. This report, along with reports of all other supervisory authorities participating in the Coordinated Enforcement Action, will result in a joint report with aggregated results, generating deeper insight and allowing targeted follow-up at EU level.

### Part I - Statistics

1. **How many stakeholders have you contacted within the following categories?**

- Ministry of the central government
- Independent public body of the central government
- Buyer for the central government
- Publicly-owned company acting as a processor for several central public bodies
- Ministry of the regional government
- Independent public body of the regional government
- Buyer for the regional government
- Publicly-owned company acting as a processor for several regional public bodies
- Other, please specify

- **Answer:** In 2022, the EDPS has formally contacted five EU institutions, bodies, offices and agencies ('EU institutions and bodies'), which could be considered equivalent to a "ministry of the central government" or "independent public body of the central government". One of those EU institutions and bodies was a buyer for other EU institutions and bodies, equivalent to a "buyer for the central government". Prior to that, all 69 EU institutions and bodies were contacted in 2020 (more on that in paragraph 35). In addition to that, several more EU institutions and bodies have been contacted informally and have been provided guidance.

---

6 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) *(OJ L 119, 4.5.2016, p. 1).*

7 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

8 *Facebook Ireland and Schrems (Schrems II)*, C-311/18, ECLI:EU:C:2020:559.

**2. How many stakeholders have you contacted within the following sectors?**

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government
- Economic affairs
- Education
- Finance
- Health
- Infrastructure
- Employment
- Justice
- Tax
- Other, please specify

- **Answer:** The EDPS has formally contacted five stakeholders in the digitalisation of the public administration/e-government and justice sectors and one stakeholder in all other listed sectors.

**3. If you have contacted a buyer, for which sectors does this buyer provide its services:**

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government
- Economic affairs
- Education
- Finance
- Health
- Infrastructure
- Employment
- Justice
- Tax
- No specific sector
- Other, please specify

- **Answer:** The buyer provides its services for all of the listed sectors.

**4. If you have contacted a buyer, and if you have this information, please specify the number of stakeholders this buyer provides services for.**

- **Answer:** The buyer provides its services to up to 71 stakeholders.

**5. What was the initial procedural framework of your action?**

- ***Fact finding***
- ***Fact finding + determining follow-up action based on the results***
- ***New investigation***[9]
- ***Ongoing investigations***

- **Answer:** At the launch of the 2022 Coordinated Enforcement Action, we were conducting ongoing investigations.

[9] Making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred.

6. **How many stakeholders indicated that they use CSPs or are planning to do so in the near future (end of 2022)?**

- **Answer:** In the context of the 2020 reporting exercise, 20 stakeholders indicated that they used or planned to use cloud service providers ('CSPs'). We assume that this number has increased since then. In particular, we note that the inter-institutional contracts with the CSPs concluded by the central buyer allow all EU institutions and bodies to use the cloud-based services under those contracts.

7. **Of the stakeholders that use CSPs (or are planning to do so in the near future), how many use CSPs for the following functions?**

- Internal organisation (office suites, internal communication, HR, etc.)
- Exercise of public functions (services to citizens, processing citizen's data, etc.)

- **Answer:** All of those stakeholders use CSPs for those two functions, i.e. at least 20 stakeholders (see our response to the preceding question). We note also that the inter-institutional contracts with the CSPs concluded by the central buyer do not make the distinction between those two functions.

8. **For the following commonly identified sectors, please specify if any hyper-scalers[10] are involved (if so please name them) either because they provide the services themselves or because the services are using the infrastructures of these hyper-scalers.**

- Health
- Finance
- Tax
- Education
- Central buyers or providers of IT services

- **Answer:** Yes, Microsoft, Amazon, IBM, OVH for all those sectors.

9. **How many stakeholders took the following actions prior to or during the acquisition of a CSP?**

- Perform a DPIA
- Does the DPIA analyse transfers in details (sometimes called DTIA)
- Contact the DPO for advice
- Perform a general risk analysis
- Contact the SA for advice

- **Answer:** Five EU institutions and bodies have performed a DPIA, contacted the DPO for advice and performed a general risk analysis. Four of those carried out a transfer impact assessment and contacted the EDPS for advice. This is without prejudice to our assessment whether those actions were performed properly.

10. **How many stakeholders (including buyers) take the following actions during the use of the CSP?**

- Monitoring technical and organisational measures to ensure compliance

[10] Hyper-scalers provide cloud services at scale. It refers usually to the big cloud providers (Google, AWS, Microsoft …) on which other services may also depend

- In case of transfers, adopting technical and organisational measures, including supplementary measures, where needed, and monitoring if changes in the regulatory landscape occur (e.g. Schrems II)
- Regular risk assessments

- **Answer:** Five EU institutions and bodies have taken the listed actions. This is without prejudice to our assessment whether those actions were performed properly.

## Part II - Substantive issues

### 1. Purpose limitation

- One of the key concerns focused on by the ongoing investigations related to the use of the CSPs is to determine whether the principle of purpose limitation has been properly respected, both contractually and in practice. This includes an examination of compliance with Articles 4(1) (b), 6 and 29(3) EUDPR (equivalent to Articles 5(1)(b), 6(4) and 28(3) GDPR). Moreover, compliance with Article 9 EUDPR, which does not have an equivalent provision in the GDPR, is also scrutinised. That provision permits the transmissions of personal data within the EEA only where this is necessary for a specific purpose in the public interest or for the performance of a task in the public interest.

- In this regard, the investigations seek to establish whether:
  - the purposes for the collection of personal data are explicit and specified and set out in a contract or another legal act;
  - the purposes for further processing are compatible with the purposes for which the data were initially collected;
  - contractual determination of categories of personal data is sufficient so as to allow the purpose for the collection and further processing to be explicit and specified.

- The issue of compliance with the principle of purpose limitation was already the subject of an EDPS investigation in 2019-2020, which concluded with the EDPS making several recommendations (see paragraph 34). The purpose of ongoing investigations is to determine whether those recommendations have been followed as well as to examine compliance related to additional CSPs used by EU institutions and bodies.

- One of the reasons for this and other compliance issues appears to be an imbalance of power between the hyper-scale CSPs and the EU institutions and bodies. In addition, the EU institutions and bodies are in some instances unable to obtain sufficient information in order to carry out proper assessments necessary for the performance of the processing and for the implementation of the required organisational and technical measures (e.g. due to business secrets invoked by certain CSPs).

- As regards differences between the stakeholders, we note that compliance levels are often higher where the EU institutions and bodies have involved the EDPS at an early stage, preferably prior to the initiation of the procurement procedure. This generally applies to all substantive issues.

- EU institutions and bodies concluding agreements with CSPs should ensure that the personal data are sufficiently determined in relation to the purposes for which they are processed and that they are collected for explicit and specified purposes and not further processed for incompatible purposes. This should be done by way of clear and exhaustive provisions stipulated in a contract

concluded pursuant to Article 29(3) EUDPR (Article 28(3) GDPR), as well as organisational and technical measures, as necessary.

**2. Controller-processor relationship**

- Another key issue is the contractual allocation of the roles of controller and processor, and in particular, whether it corresponds to the factual circumstances. This entails an examination of compliance with Articles 29 and 30 EUDPR (equivalent to Articles 28 and 29 GDPR).

- The ongoing investigations focus on whether the divisions between the roles is appropriately defined in light of the public service character of EU institutions and bodies. As such, the EU institutions and bodies should ensure that the factual circumstances of the processing, including the determination of its purposes and means, are accurately reflected in the allocation of the roles and corresponding responsibilities under the relevant contracts.

**3. Authorisation AND USE of sub-processors**

- A related issue under examination concerns the engagement and use of sub-processors as regulated by Article 29(1), (2) and (4) EUDPR (equivalent to Article 28(1), (2) and (4) GDPR). This may also result in an infringement of Article 29(3) (d) EUDPR (equivalent to Article 28(3) (d) GDPR). In particular, the investigations seek to establish whether the EU institutions and bodies as controllers have:

    - a meaningful right to withhold authorisation of sub-processors;
    - authorised only the use of sub-processors which provide sufficient guarantees within the meaning of Article 29(1) EUDPR (equivalent to Article 28(1) GDPR);
    - ensured that the contract between the processor and sub-processors sets out the same data protection obligations, as they must be stipulated in the contract between the controller and processor, as required by Article 29(4) EUDPR (equivalent to Article 28(4) GDPR).

- The solutions depend on the specific circumstances of each case, however one potential solution for a controller seeking to gain greater control over the selection of the sub-processors by hyper-scale CSPs might be to define contractually the specific criteria that any new sub-processors must meet, or to define what information the CSPs must provide on proposed new sub-processors. This could allow controllers to anticipate and mitigate risks posed to data subjects better.

**4. Technical and security measures to mitigate risks**

- Our investigation further seeks to establish whether appropriate security measures of technical and organisational nature have been identified in the controller's security risk assessment and whether they have been made mandatory with respect to all applicable processing operations.

- Such security measures are required, in particular, by Article 33 EUDPR (equivalent to Article 32 GDPR) and by Article 36 EUDPR (no equivalent provision in GDPR). This includes logging, encryption, identification and authentication of users, audits events, incident handling, flaw remediation etc. Particular attention is dedicated to measures that mitigate the highest risks identified.

- In case an infringement is established, the controller should, in particular, ensure that all the necessary security measures are clearly determined as mandatory.

**5. International transfers**

- Another major area of concern is transfers outside the EEA and the requirements, in particular, of Chapter V EUDPR (similar to Chapter V GDPR) as interpreted by the Schrems II judgment. Our ongoing investigations focus mainly on:
    - the controller's understanding of what transfers are taking place, i.e. the accuracy and completeness of its transfer mapping exercises;
    - transfer impact assessment, i.e. assessing the level of protection in the third country in the context of the specific transfers as to whether supplementary measures are needed and whether any effective supplementary measures exist;
    - implementation of appropriate contractual and other safeguards, including effective supplementary measures where required.

- These issues are interlinked since they have to be properly carried out in sequence. In other words, a complete transfer impact assessment cannot be carried out without first completing proper transfer mapping, nor is it possible to implement effective safeguards without a thorough transfer impact assessment. An important element to take into account is that depending on the nature of the processing, effective supplementary measures may not be available even where they are required to ensure an essentially equivalent level of protection.

- The EUDPR/GDPR, as interpreted by the Court of Justice, do not permit transfers where required supplementary measures are not implemented. In such instances, the EU institutions and bodies should ensure that such transfers do not take place. In some cases, it may be possible to take advantage of a sovereign cloud solution which would not entail transfers outside the EEA nor the application of extra-territorial third-country legislation.

- In order to achieve compliance, the EU institutions and bodies should:
    - carry out an exhaustive transfer mapping exercise in order to identify which personal data are transferred to which recipients in which third countries and for which purposes, including any onward transfers;
    - carry out a complete transfer impact assessment;
    - implement effective safeguards and mitigating measures, including supplementary measures if any are identified in the transfer impact assessment.

- Additionally, EU institutions and bodies can assess alternatives to using a current CSP, which would not result in non-compliant transfers.

**6. <u>Necessity to use cloud-based services</u>**

- The EDPS has also been paying particular attention to compliance with the data minimisation principle referred to in Article 4(1)(c) EUDPR (equivalent to Article 5(1)(c) GDPR) as well as with data protection by design and by default principles under Article 27 EUDPR (equivalent to Article 25 GDPR) in relation to the use of CSPs. It is incumbent on the controller to choose processing activities that are the least intrusive while still being effective. As regards the selection and use of IT products and services entailing the processing of personal data, the respect for this principle would require making reasonable efforts in seeking alternatives that allow the controller to carry out its tasks effectively while posing lower risk to data subjects.

- In that regard, the controller would have to demonstrate such compliance, as required by the accountability principle referred to in Article 4(2) EUDPR (equivalent to Article 5(2) GDPR) and the controller's obligations specified in Article 26 EUDPR (equivalent to Article 24 GDPR). This implies showing that the selection of the CSP concerned was an outcome of a thorough process assessing

the existence of data protection compliant alternative products and services meeting its specific needs.

## Part III - Actions by the SA

1. **Actions taken prior to the launch of the coordinated action**

- In 2019-2020, the EDPS carried out an investigation into the use of Microsoft's products and services by EU institutions and bodies. Based on that investigation, the EDPS issued its **Findings and Recommendations** to the EU institutions and bodies.[11] This occurred before the Court of Justice handed down the Schrems II judgment, however, many of the identified issues anticipated that ruling. In particular, the recommendations pertained to ensuring that the EU institutions and bodies maintain proper control over the processing activities, particularly in view of the public role of the EU institutions and bodies, as well as control over what data are transferred where and how. Moreover, the EDPS recommended that the EU institutions and bodies put in place appropriate technical measures to stem the flow of personal data sent to the CSPs as well measures to be taken to ensure compliance with the transparency obligations of EU institutions and bodies towards data subjects.
- In the context of its Schrems II Strategy,[12] the EDPS issued an **order**, in October 2020, to all EU institutions and bodies to complete a transfer mapping exercise identifying which ongoing contracts, procurement procedures and other types of cooperation involve transfers of data, and to report certain results to the EDPS. We also strongly encouraged the EU institutions and bodies to avoid processing activities that involve transfers of personal data to the United States. Following that order, the EDPS has received numerous requests for guidance on proper compliance, which we have provided as informal and formal supervisory opinions.
- In May 2021, the EDPS opened two investigations following the Schrems II judgment.[13] One regarding the use of cloud services provided by Amazon Web Services and Microsoft under Cloud II contracts by EU institutions and bodies, and one regarding the use of Microsoft 365 by the European Commission.
- In July 2021, the EDPS issued an **opinion**[14] in response to a request for prior consultation under Article 40 EUDPR (equivalent to Article 36 GDPR) by an EU institution (the European Central Bank). In that opinion, the EDPS addressed the question whether mitigating measures identified by the institution concerned could be considered sufficient to appropriately address the high risk identified in relation to the envisaged use of Microsoft Dynamics 365. The EDPS concluded that the envisaged measures were insufficient to mitigate those risks. As a consequence, the EDPS found that there were not sufficient guarantees and appropriate safeguards that the processing by the CSP and its sub-processors would meet the statutory requirements and ensure an essentially equivalent level of protection to that guaranteed in the EEA. The EDPS therefore issued a **warning** that the envisaged processing operation was likely to infringe Articles 4(2), 27, 29, 46, and 48 EUDPR (equivalent to Articles 5(2), 25, 28, 44 and 46 GDPR). Moreover, the EDPS made several **recommendations** to assist the institution in ensuring compliant processing.

---

[11] See the EDPS Public Paper on the Outcome of own-initiative investigation into EU institutions' use of Microsoft products and services.

[12] EDPS Strategy for Union institutions, offices, bodies and agencies to comply with the 'Schrems II' Ruling.

[13] https://edps.europa.eu/press-publications/press-news/press-releases/2021/edps-opens-two-investigations-following-schrems_en.

[14] EDPS Opinion on a prior consultation requested by the European Central Bank on their new customer relationship management system.

- In July 2021, the EDPS issued another **opinion**[15] in relation to transfers to a third country. The opinion included guidance on the use of derogations under Article 50 EUDPR (similar to Article 49 GDPR) for transfers carried out in the context of the use of the CSP for the purposes of publishing a newsletter by the EU agency (ENISA). In particular, we highlighted that the agency should assess, in cooperation with the CSP, whether there were alternative newsletter publishing solutions available that do not involve the transfers of personal data to the United States.

**2. Actions envisaged or taken after the launch of the coordinated action**

- In April 2022, the EDPS published a **factsheet**[16] in order to share an informal supervisory opinion issued to an EU institution requesting guidance. In that document, the EDPS reminded the EU institutions and bodies of the recommendations issued following its 2019-2020 investigation into the use of Microsoft's products and services by EU institutions and bodies and of its ongoing investigation into the use of Microsoft 365 by the European Commission. The EDPS also recalled the requirements and consequences of the Schrems II judgment as regards the transfers outside the EEA as well as informed them of the 2022 Coordinated Enforcement Action.
- In April 2022, the EDPS also issued a **decision**[17] to an EU agency (Frontex) on its move to a hybrid cloud consisting of Microsoft Office 365, Amazon Web Services (AWS) and Microsoft Azure, following an investigation initiated in June 2020. The investigation looked at compliance with the EUDPR, taking into account EDPS Guidelines on the use of cloud computing services[18] issued in 2018. The EDPS found that the agency had moved to the cloud without a timely and exhaustive assessment of data protection risks and identification and implementation of appropriate mitigating measures. The EDPS also found that the agency had failed to observe the principles of lawfulness and data minimisation. The EDPS therefore issued a **reprimand** for a breach of Articles 4(2), 26 and 27 EUDPR (equivalent to Articles 5(2), 24 and 25 GDPR) as well as an **order** to review and amend the DPIA and the record of processing activities to bring the processing into compliance with the EUDPR.
- In June 2022, the EDPS issued an **opinion** to an EU agency in response to a request for prior consultation on an online platform entailing the use of cloud computing services. The EDPS concluded that the specific risks related to the development and operation of the online platform had not been sufficiently identified. In particular, it recommended that the agency ensure that the contractual framework binds the processor to meet the data protection requirements and that it assess the transfers that the use of cloud services may entail.
- In October 2022, the EDPS issued a decision pursuant to Article 58(3) (e) EUDPR (equivalent to Article 58(3) (h) GDPR) conditionally authorising the use of contractual clauses for transfers of personal data between an EU institution (the Court of Justice of the EU) and a CSP (Cisco). The EDPS authorised their use until 31 October 2024 given, inter alia, the essential function that the institution carries out in the EU, the commitment by the institution and the CSP to comply with the EUDPR and the need for a certain period of time to implement the necessary measures. However, the EDPS set a number of strict conditions to be met in order to remedy the remaining shortcomings and to ensure an essentially equivalent level of protection. This decision follows a

[15] EDPS Opinion on transfers to a third country resulting from the use of a newsletter service by ENISA.
[16] https://edps.europa.eu/system/files/2022-04/22-04-29_ongoing-investigation-into-the-use-of-m365-by-euis_en.pdf.
[17] EDPS Decision concerning the investigation into Frontex's move to the Cloud.
[18] EDPS Guidelines on the use of cloud computing services by the European institutions and bodies.

previous EDPS decision of August 2021[19] authorising the use of the contractual clauses in question for 13 months.

- Furthermore, in addition to pending requests for prior consultation, the EDPS intends to issue decisions once the ongoing investigations have been concluded, and use its corrective powers where necessary. It is envisaged to issue those decisions in 2022/2023.

## Part IV - Other

### 1. General impression

- The levels of awareness and compliance appear to be relatively low. However, we have reasons to presume that following the EDPS' order of 2020 to carry out a transfer mapping exercise to all EU institutions and bodies, as well as further guidance provided, the overall awareness and compliance in that regard have risen. Nonetheless, the need for improvement remains, in particular as regards the proper implementation of measures that will, in addition to contractual measures, mitigate the risks arising from third-country legislation.

### 2. Leading practices

- The EDPS (as a supervisory authority) and other EU institutions and bodies (as controllers) have been closely involved in certain inter-institutional procurement procedures[20] relating to the cloud services. This has allowed the relevant data protection and security requirements to be integrated already in the procurement notice and selection and were therefore reflected in the subsequent contracts. Since many data protection issues stem already from the procurement stage, such practice effectively contributes to the proper implementation of the relevant rules. The EU institutions and bodies that were already closely involved in such procedures before Schrems II judgment, have become even more involved following that judgment. In particular, this concerns greater involvement in clarifying the situations in which cloud services may be used and what safeguards and measures are already available, as well as in the development of new measures additional to those already in place.
- In addition, the EDPS as a controller initiated an informal consultation concerning the procurement of Software-as-a-Service and hosting services from an EU-based provider. The EDPS as a supervisory authority made recommendations to the controller on data protection requirements within the procurement procedure, on the selection of providers by using relevant data protection criteria and guarantees to be required from the provider, including ensuring that processing only takes place in the EEA and that extra-territorial third-country legislation does not apply. Furthermore, we advised the controller on technical, organisational and security measures to be implemented, additional contractual clauses to be included into the model inter-institutional contract to be led by the EDPS, and on the involvement of other EU institutions and bodies. Following the procurement procedure, the SaaS will be based on Nextcloud's software and will be provided and hosted by TAS France.
- The EDPS also welcomes the requests of EU institutions and bodies for guidance, as well as requests for prior consultation or authorisation where required in accordance with the relevant statutory provisions. Such requests of EU institutions and bodies are an indication of an elevated level of awareness of the impact that the processing in the cloud and international transfers have on individuals. This is a crucial step towards compliance with the applicable EU data protection law.

---

[19] EDPS Decision authorising temporarily the use of ad hoc contractual clauses between the Court of Justice of the EU and Cisco for transfers of personal data in the Court's use of Cisco Webex and related services.

[20] Both before and after the Schrems II judgment.

# EE SA

## Estonian Data Protection Inspectorate

### Part I – Statistics

1. **How many stakeholders have you contacted within the following categories?**

- Ministry of the central government: **1**
- Independent public body of the central government: **2**
- Buyer for the central government: **n/a**
- Publicly-owned company acting as a processor for several central public bodies: **n/a**
- Ministry of the regional government: **n/a**
- Independent public body of the regional government: **1**
- Buyer for the regional government: **n/a**
- Publicly-owned company acting as a processor for several regional public bodies: **n/a**
- Other, please specify: **n/a**

2. **How many stakeholders have you contacted within the following sectors?**

- Agriculture: **n/a**
- Defence: **n/a**
- Digitalisation of the Public Administration/e-Government: **n/a**
- Economic affairs: **n/a**
- Education: **1**
- Finance: **n/a**
- Health: **1**
- Infrastructure: **1**
- Employment: **n/a**
- Justice: **n/a**
- Tax: **n/a**
- Other, please specify: **1 municipality**

3. **If you have contacted a buyer, for which sectors does this buyer provides its services:**

- n/a

4. **If you have contacted a buyer, and if you have this information, please specify the number of stakeholders this buyer provides services for:**

- n/a

5. **What was the initial procedural framework of your action?**

- Fact finding
- Fact finding + determining follow-up action based on the results
- New investigation[21]
- Ongoing investigation

6. **How many stakeholders indicated that they use CSPs or are planning to do so in the near future (end of 2022)?**

- All 4 stakeholders indicated that they use CSPs.

[21] making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred

7. **Of the stakeholders that use CSPs (or are planning to do so in the near future), how many use CSPs for the following functions?**

- Internal organisation (office suites, internal communication, HR, etc.) : **3**
- Exercise of public functions (services to citizens, processing citizen's data, etc.): **4 (all responding stakeholders).**
-

8. **For the following commonly identified sectors, please specify if any hyperscalers[22] are involved (if so please name them) either because they provide the services themselves or because the services are using the infrastructures of these hyper-scalers**

- Health: **Microsoft, Fujitsu**
- Finance: **n/a**
- Tax: **n/a**
- Transport: **Microsoft, Amazon**
- Education: **Microsoft, Google, Adobe, Zoom, Facebook, Instagram**
- Central buyers or providers of IT services: **n/a**

9. **How many stakeholders took the following actions prior to- or during the acquisition of a CSP?**

- Perform a DPIA: **1**
- Does the DPIA analyse transfers in details (sometimes called DTIA): **Content of the DPIA is unknown, as it was not asked to submit.**
- Contact the DPO for advice: **3**
- Perform a general risk analysis: **based on stakeholder's answers, we are not aware (or can`t be sure) that written risk analysis (from the point of data processing) are performed.**
- Contact the SA for advice: **0**

10. **How many stakeholders (including buyers) take the following actions during the use of the CSP?**

- Monitoring technical and organisational measures to ensure compliance: **4**
- In case of transfers, adopting technical and organisational measures, including supplementary measures, where needed, and monitoring if changes in the regulatory landscape occur (e.g. Schrems II): **0. As a rule of thumb, stakeholders rely on CSP standard agreement and SLA terms. No supplementary measures are adopted and regulatory landscape is not monitored. Only one stakeholder mentioned that CSP has implemented SCC (EC 2021/914). Stakeholders experience lack of awareness if and which personal data might be transferred to third country.**
- Regular risk assessments: **based on answers we cannot be sure that regular risk assessment is performed.**

## Part II – Substantive issues

- The Supervision Authority participated in the joint surveillance of the EDPB in the form of fact finding monitoring. The aim was, in particular, to map the practice of using public cloud services in selected institutions and to what extent the authorities have understood the impact of the use of cloud services on data protection and people's privacy. We have had no further contact with the data controllers following the answers to the questions. We may start with follow-up activities

[22] Hyper-scalers provide cloud services at scale. It refers usually to the big cloud providers (Google, AWS, Microsoft …) on which other services may also depend

in the beginning of next year. As a result, no solutions and corrective actions could be implemented yet in relation to the issues raised by the monitoring.

- The responses to the monitoring exercise identified the following potential problems and bottlenecks:

**1. <u>Data processors lack clarity on whether and what personal data are processed in cloud services and to what extent</u>**

- Understanding the processing of personal data and its scope is one of the most important components of legitimate applicability of the GDPR. If personal data is not processed in the information systems, the GDPR does not apply. If personal data exists, the scope of applicability of the GDPR depends, for example, on the sensitivity of the data, the volume of the data or whether the systems processing the data are located in third countries. The context is therefore of paramount importance.

- Three out of four respondents made it clear that personal data is processed in cloud services. Of these, only two authorities indicated that the data of both employees and other persons (publicity) are processed in cloud services. One authority's reply gave the impression that only data from cloud administrators is processed. The information was also contradictory at times because, for example, for the question of whether DPIA was also carried out, there were responses that since the volume of personal data processed is currently small, DPIA was not deemed necessary.

- According to one of the respondents, there are also special categories of personal data among the data processed.

- According to one of the respondents, data processed in cloud services only concerns employees. However, it is difficult to accept this argument as the service used included, for example, MS 365, Google, Zoom and Facebook. If an institution uses e.g. cloud-based office software, the documents that are to be processed or compiled certainly do not contain only staff-related data. The authorities also communicate very much with public in the context of their public tasks. On a daily basis, individuals also turn to authorities with various problems and questions. Often these are sensitive issues of individuals, including minors.

**2. <u>No data protection impact assessment has been carried out prior to the use of cloud services</u>**

- This is a major problem for all respondents. Common reasons why no impact assessment was made were that there was no personal data; that the service provider had already done so and trusted it; or that it was not a high-risk data processing. Only one of the respondents said they had done it. However, since there was no obligation to transmit impact assessment documents in the context of the monitoring, it is difficult for us to say whether the impact assessment had been carried out in accordance with the requirements of Article 35 GDPR.

- It is important to note that if an impact assessment has been carried out by any cloud service provider, this is usually an analysis of the overall risks. Often only from the viewpoint of information security and information system as a whole. However, the potential risks of data protection for the people involved in the service have not been assessed. After all, the service provider is not aware of the organizational or national legal obligations of the body using the service.

- It was also clear from the answers that when entering the service, the first priority of the institution was to find solutions primarily for organizational needs. Often the only goal is to save the costs to infrastructure and optimization.

**3. <u>The use of the service is based on the service provider's standard contract and the service level agreement (SLA)</u>**

- According to only one respondent, there was the impression that the institution had pre-contractual negotiations with the service provider. An adapted SLA is also concluded if the SLA by the service provider does not meet the expectations. Allegedly, the institution has the right to control and audit the cloud service provider under the contract.

- The remaining three respondents rely on the service provider's standard terms of the contract. Thus, the authorities have generally failed to comply with the requirement of Article 28 of the GDPR. However, in the case of unilateral acceptance of the contract terms of the service provider, it is difficult for the authorities to ensure compliance with other provisions of the GDPR, for example with Articles 5, 12, 13, 14, 21, 24, and 32 of the GDPR. The service provider may contractually assume the rights to process datasets relating to the activities of the institution for its own purposes. Often, these goals are deliberately formulated in such a general way that the understanding of what a cloud enterprise actually does and how much a cloud enterprise does is incomprehensible. Authorities take very lightly the service provider's claims that the contract complies with GDPR requirements.

**4. <u>Lack of awareness of sub-delegated processors</u>**

- As a general rule, all cloud services use external partners, i.e. sub-processors, who process data on the basis of the processor's authorization pursuant to Article 29 of the GDPR. Be it to ensure a component or a function of the service. This is particularly relevant in ensuring information security, where different firewall solutions or distribution of network loads are carried out by external parties. Therefore, it is of paramount importance for the authority using cloud service, as responsible for compliance with GDPR requirements, to understand and know which parties are involved in data processing.

- Monitoring confirmed our practice so far that the knowledge of data processors in sub-delegated processing is lacking or none. Three out of four respondents said they did not know which sub-processors are being used by the cloud service provider. One respondent claimed that sub-processors were not used (although they were the two largest cloud services in the world). Only one respondent provided a list of sub-processors in the cloud service provider's contract.

- In the case of sub-processors, the lack of knowledge of the region in which the data processing is carried out is also a major problem. This can occur in third countries. Despite the lack of knowledge of sub-processors by controllers, the sub-processor under Article 29 GDPR is obliged to process the data under the instructions of the controller.

**5. <u>Lack of awareness of telemetry/diagnostic data processing</u>**

- Only one out of four respondents indicated that cloud services do not process telemetry or diagnostic information. The other three replied that such processing takes place, but the data processed does not include personal data. The reason was to ensure the quality of the service or to identify errors. Two respondents were aware that, in the context of the processing of cloud telemetry data, data transfers to third countries take place on the basis of Chapter V of the GDPR.

6. **Insufficient due diligence in implementing additional safeguards for transfers to a third countries**

- According to the three respondents, there is no transfer to third countries, as they rely on the cloud service provider's confirmation and the possibility to select a data centers in the European Union for data processing. Only one respondent says that data transfer to third countries is taking place. According to the same respondent, the cloud service provider uses standard contractual clauses under Commission Implementing Decision 2021/914. It is not specified whether the contract is the controller-processor or the processor-processor.

## Part III – Actions by the SA

1. **Have you taken action (i.e. fact-finding exercises, informal contact, prior consultation, investigation) towards any of the stakeholders concerning the use of cloud-based services prior to launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

- No, we haven't taken any action towards any of the stakeholders concerning the use of cloud based services prior to launching the coordinated action.

2. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (E.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**

- Specific actions are not planned yet. It would be under discussion which are our focus topics for 2023 work plan.

## Part IV – Other

1. **What is your general impression of the levels of awareness and compliance of the stakeholders you consulted concerning the use of cloud?**

- Based on sweep answers we have received, level of awareness and compliance of the stakeholders is not sufficient.

2. **Are there any other issues or topics that you would like to flag?**

- In Estonia, the legal framework for the use of public cloud services in the public sector are being prepared by the Ministry of Economic Affairs and Communications.

3. **Are there any leading practices of the stakeholders you have contacted that you would like to share?**

- No

# EL SA

## Hellenic Data Protection Authority

### Part I – Statistics

1. **How many stakeholders have you contacted within the following categories?**

- Ministry of the central government : **3**
- Independent public body of the central government : **4**
- Buyer for the central government : **1 (the buyer is a ministry of the central government – Ministry of Digital Governance and is included in the number above for the ministries contacted)**
- Publicly-owned company acting as a processor for several central public bodies
- Ministry of the regional government
- Independent public body of the regional government
- Buyer for the regional government
- Publicly-owned company acting as a processor for several regional public bodies
- Other, please specify

2. **How many stakeholders have you contacted within the following sectors?**

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government : **1**
- Economic affairs
- Education
- Finance
- Health : **2**
- Infrastructure
- Employment : **3**
- Justice
- Tax
- Other, please specify : **Immigration and Asylum : 1**

3. **If you have contacted a buyer, for which sectors does this buyer provides its services:**

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government
- Economic affairs
- Education
- Finance
- Health
- Infrastructure
- Employment
- Justice
- Tax
- No specific sector: **The Ministry of Digital Government offers cloud services through the governmental Cloud (G-Cloud) to public bodies of every sector.**
- Other, please specify

4. **<u>If you have contacted a buyer, and if you have this information, please specify the number of stakeholders this buyer provides services for:</u>**

- Approximately 150 public bodies are hosted in G-Cloud (information taken from the buyer's website: https://www.gsis.gr/ggpsdd/orama-apostoli)

5. **<u>What was the initial procedural framework of your action?</u>**

- Fact finding
- Fact finding + determining follow-up action based on the results: **The initial framework was fact finding and determining follow-up action based on the results**
- New investigation[23]
- Ongoing investigation

6. **<u>How many stakeholders indicated that they use CSPs or are planning to do so in the near future (end of 2022)?</u>**

- All 7 of them (the 5 stakeholders contacted and 2 more, for which the Ministry of Labour and Social Affairs also sent answers to the questionnaire)

7. **<u>Of the stakeholders that use CSPs (or are planning to do so in the near future), how many use CSPs for the following functions?</u>**

- Internal organisation (office suites, internal communication, HR, etc.) : **6**
- Exercise of public functions (services to citizens, processing citizen's data, etc.) : **7**

8. **<u>For the following commonly identified sectors, please specify if any hyperscalers[24] are involved (if so please name them) either because they provide the services themselves or because the services are using the infrastructures of these hyper-scalers</u>**

- Health: **Yes (Microsoft)**
- Finance: **Yes (Oracle, Microsoft 365)**
- Tax: **Yes (Oracle, Microsoft Azure, Microsoft 365)**
- Education
- Central buyers or providers of IT services: **Yes (Microsoft, Oracle)**
- Other: **Employment (Amazon)**

9. **<u>How many stakeholders took the following actions prior to- or during the acquisition of a CSP?</u>**

- Perform a DPIA : **1**
- Does the DPIA analyse transfers in details (sometimes called DTIA) : **Yes**
- Contact the DPO for advice : **3**
- Perform a general risk analysis: **None**
- Contact the SA for advice: **None**

10. **<u>How many stakeholders (including buyers) take the following actions during the use of the CSP?</u>**

- Monitoring technical and organisational measures to ensure compliance: **2**
- In case of transfers, adopting technical and organisational measures, including supplementary measures, where needed, and monitoring if changes in the regulatory landscape occur (e.g. Schrems II). : **None**

[23] making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred

[24] Hyper-scalers provide cloud services at scale. It refers usually to the big cloud providers (Google, AWS, Microsoft …) on which other services may also depend

– Regular risk assessments : **2**

## Part II – Substantive issues

**1. Lack of a general risk assessment and/or DPIA**

**1.1. Short description:**

- According to the questionnaire replies, the CSPs are selected as processors or sub-processors without a general risk assessment.

- With one exception, the questionnaire respondents have not carried out a DPIA or have not asked for a DPIA from the CSP prior to acquiring cloud-based services. Regarding the exception, one public body performed DPIAs for two (2) separate systems after the CSP selection. In this case, the first DPIA has not examined the risks arising from the use of cloud services, while the second suggests specific measures to minimize the risks associated with the use of cloud services, but it is not clear if the controller has taken such measures.

- For the selection of the Government Cloud (G-Cloud) (without a DPIA), a common reason put forward by public bodies is the mandatory use of G-Cloud according to Law 4727/2020 Art. 87 par.4 (as amended)[25]. Another reason put forward by one public body is the processing of a very limited amount of special categories of personal data. Other reasons include the Tier-3 architecture of G-Cloud and its preparation for the acquisition of the ISO 27001 certification.

- In the case of the hyper-scalers, the reasons for their selection include the following: ease of use, expertise and high technological solutions provided, the certifications that hyper-scalers possess (for Microsoft ISO 27001, 9001, 27017, 27018, 27701, 22301 and for Oracle ISO 27001, 27017, 27018, and 27701).

**1.2. Which provisions of the GDPR this concerns:**

- Articles 24, 28 and 35 GDPR

**1.3. Why this has been an issue for the stakeholders :**

- The lack of a general risk assessment and/or a DPIA, where necessary, results to the inability of stakeholders to identify and effectively address the risks related to the processing of personal data in the use of cloud services. This deficiency, together with the lack of awareness suggests that stakeholders may face difficulties fulfilling their accountability obligation to use only processors providing sufficient guarantees, according to Art. 28 (1) GDPR.

**1.4. Differences between stakeholders:**

- Most of the public bodies our SA contacted have not performed any kind of risk assessment before or after acquiring a CSP. Only one public body has carried out DPIAs in two cases with the specific issues as described above.

**1.5. Potential solutions to this issue by the SA or the stakeholders:**

[25] "*All central electronic applications and central information systems maintained by all Ministries […] public entities […] independent authorities […etc.] which concern transactions with natural or legal persons or legal entities and the public administration, must be installed in the Public Sector Government Cloud by 1st January 2023. The Government Cloud (G-Cloud) infrastructures of the above entities are transferred and become the property of the General Secretariat of Information Systems for Public Administration for this purpose*".

- A possible solution for the stakeholders would be to carry out a DPIA, at least "ex post" on the use of cloud services, in order to determine any necessary supplementary technical and organizational measures. Another possible solution would be for the central buyer to perform a basic DPIA as a whole, taking into account Law 4727/2020 Art. 87 par.4 (as amended).

**2. Not fully clear role of the parties, including resellers and intermediaries**

**2.1. Short description:**

- There is not a common understanding among the stakeholders about the roles of the parties involved in the use of cloud services.

- According to most questionnaire responses, the public bodies act as controllers and the CSPs (central buyer, hyper-scalers) as processors or sub-processors. In some cases, public bodies consider the central buyer to be an independent data controller or a joint controller, because it has the ability to decide on the means of the processing and the selection of sub-processors for providing the G-Cloud services[26].

- The central buyer itself reported that it acts as processor for providing the G-Cloud services to public bodies, with hyper-scalers (Microsoft, Oracle) as sub-processors for cloud services.

- The role of the hyper-scalers is also not clear regarding the processing of telemetry/diagnostic data that takes place for their own purposes. One public body considered to be a joint controller with Microsoft for the use of Office 365 Suite, because the CSP decides independently on the means of the processing but when our SA asked for further clarifications, this body changed its opinion and answered that Microsoft is a processor.

- The contracts submitted to our SA revealed various relationships. One public body submitted a Microsoft Business and Service Agreement signed between the public body and Microsoft Ireland Operations Limited incorporating the Microsoft Products and Services Data Protection Addendum (DPA) by reference. In another case, the hyper-scaler Amazon Germany is the sub-processor of a consulting company acting as processor for the public body, but without in fact offering cloud services itself (indirect involvement with the hyper-scaler).

- In the other cases with hyper-scaler involvement (Oracle, Microsoft), a contract exists between the controller (direct involvement) or processor (indirect involvement) and the reseller of the hyper-scaler. The reseller is selected through a public procurement procedure and the contract is established after the selection. The role of the reseller (according to the provisions of the GDPR) is not clear and not defined in the contract. It is evident from the questionnaire responses that the role of the resellers/intermediaries is not known to all public bodies.

**2.2. Which provisions of the GDPR this concerns:**

- Articles 4 (7), (8), 26, 28.1 GDPR

[26] According to article 85 of law 4727/2020, among the responsibilities of the central buyer is to acquire cloud services, in total for all public bodies, by priority relative to other technological solutions, for several purposes including the provision of cloud services to public bodies. Also, according to article 28 par. 3 of law 4623/2019, the central buyer is responsible, among others, for the design, development, extension and productive operation of central Governmental Cloud infrastructures, in total for all Public Administration, with the goal of hosting all applications in the central G-Cloud infrastructures of public administration.

**2.3. Why this has been an issue for the stakeholders:**

- Without clear roles of the parties involved, the public bodies are unable to identify and fulfill their responsibilities arising from the GDPR. The contracts between the parties might miss important elements regarding the processing of personal data or even include incorrect ones. The selection of the CSP becomes difficult, as it is not clear, which party has the responsibility to perform a general risk assessment and decide the selection criteria. In case data subjects exercise their rights regarding data processing in the cloud, the public bodies might not be able to respond to them appropriately. They might also not be able to fulfill their accountability obligation or respond accordingly to the SA.

**2.4. Differences between stakeholders:**

- The differences between stakeholders are presented in the short description above.

**2.5. Potential solutions to this issue by the SA or the stakeholders:**

- The roles of the involved parties should be clearly and unequivocally determined and precisely defined in the contract. To this end, public bodies should clearly establish their role relative to the use of cloud services, possibly through an internal assessment. In addition, adequate information from the CSP and DPO consultancy are important elements so that stakeholders become aware of their responsibility and be able to distinguish and evaluate properly their roles in the processing in order to select a CSP according to the provisions of the GDPR.

**3. Difficulty in negotiating or changing terms of the contract with the CSP**

**3.1. Short description:**

- The questionnaire replies revealed difficulty of public bodies in negotiating terms or changing the terms of the contract with the CSPs. The terms of the contract are usually predetermined by the CSP.

- The answers provided to the questionnaire regarding the contract with the CSP merely quote parts of Microsoft's DPA, thus indicating either lack of knowledge by stakeholders and/or difficulty in negotiating terms.

- Regarding the possibility of termination or reversibility of the contract, most stakeholders refer to Microsoft's standard terms or answer negatively (either it has not been checked by the public body or such a possibility is not provided). Only one stakeholder answered positively without further explanation.

- The DPA contains information on the processing that Microsoft undertakes as a processor. The DPA is incorporated into the (volume or enterprise) licensing agreement and applies to each customer, irrespectively of products or services. This standard DPA may not suffice as the contract envisaged in article 28 GDPR. More precisely, the DPA Statement that "*the Customer's licensing agreement, including the DPA Terms, along with the product documentation and Customer's use and configuration of features in the Products, are Customer's* (as a Controller) *complete documented instructions to Microsoft* (as a Processor) *for the processing of Personal Data",* is too generic and vague to constitute the documented instructions of Article 28(3) GDPR. Moreover, the categories of personal data ("*data generated, derived or collected by Microsoft, including data sent to Microsoft as a result of a Customer's use of service-based capabilities or obtained by*

*Microsoft from locally installed software*"[27]) and the purposes for which Microsoft acts as an independent data controller are very broad and not sufficiently explained.

The same applies regarding Oracle as processor. The Data Processing Agreement for Oracle Services incorporates the European DPA Addendum which makes reference to the Oracle Processor Code (Binding Corporate Rules for Processors) regarding cross-border data transfers[28]. The Oracle Privacy Code applies to "*Personal Information of Customer Individuals subject to EEA Data Protection Laws and Processed by Oracle on behalf of its Customers in its role as a Processor in the course of delivering Services*".[29] The above are standard common documents and apply to all controllers independently of the specific processing. For example, it is not clear and sufficiently explained why and when it is necessary for Oracle to collect data about customer end users, employees, job applicants, end-customers and clients for its own purposes.

**3.2. <u>Which provisions of the GDPR this concerns:</u>**

- 26, 28 (1), 28 (3), 29

**3.3. <u>Why this has been an issue for the stakeholders:</u>**

- In many cases, CSPs keep a level of control over the processing that may exceed the role of the processor. If the public bodies have no chance to negotiate such terms, it may be difficult for them to keep determining the purposes and the means over the processing of personal data, and therefore they may not be able to fulfill their obligations as controllers, according to the accountability principle.

**3.4. <u>Differences between stakeholders:</u>**

- The differences are as described above. Generally, there have been no significant differences found, about the fact that most answers were copied directly from the CSPs standard texts.

**3.5. <u>Potential solutions to this issue by the SA or the stakeholders:</u>**

- A possible solution would be to investigate whether there is a possibility for public bodies to engage into negotiations with the CSPs, in order to change or insert specific provisions in the contract, with the aim of retaining control over personal data processing and in case this is not feasible, to consider choosing another CSP.

**4. <u>Lack of a contract or other legal act according to Art. 28/26 GDPR</u>**

**4.1. <u>Short description:</u>**

- According to the questionnaire replies provided by the participating public bodies, a contract or other legal act, pursuant to article 28(3) GDPR, has not been established between each of them and the central buyer.

- In two cases, the contract with the reseller contains an Appendix for the protection of personal data, pursuant to Art. 28 (3) GDPR. However, in two other cases, the contract with the reseller

[27] https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA

[28] According to Oracle: '*Oracle's BCR-p (also called the 'Oracle Processor Code') has been integrated into a **new European DPA Addendum**, which was added to the new DPA. The European DPA Addendum bundles all GDPR-specific information requirements for data processing agreements, while the DPA describes the general processing terms for all customer personal information globally'*. (Source: https://www.oracle.com/be/a/ocom/docs/corporate/dpa-bcr-statement-of-changes-062619.pdf)

[29] https://www.oracle.com/a/ocom/docs/corporate/bcr-privacy-code-051719.pdf

refers explicitly to specific future agreements/contracts, to fulfill the requirements of Art. 28(3) GDPR, but such contracts were not presented to our SA.

- In all cases with a reseller contract, none of the stakeholders has submitted to our SA an SLA or a licensing agreement with the hyper-scaler. So, this part of the relationship is missing.

**4.2. Which provisions of the GDPR this concerns:**

- Articles 24, 26, 28 (3) GDPR

**4.3. Why this has been an issue for the stakeholders:**

- Without a proper contract or other legal act in place, the processing on behalf of the controller is not adequately determined. This deficiency makes it difficult for the public bodies to comply with their obligation arising from Art. 28 (1) GPDR, to "*use only processors providing sufficient guarantees"* that the processing meets the requirements of the GDPR.

**4.4. Differences between stakeholders:**

- The differences between stakeholders are presented in the short description above. Overall, no differences were identified among respondents in that they all referred to the standard, predetermined terms of the CSPs. In addition, no differences were found among the participating public bodies concerning the lack of a contract/other legal act with the central buyer as processor containing the terms described in Art. 28.3 GDPR.

**4.5. Potential solutions to this issue by the SA or the stakeholders:**

- In the cases where the contract refers to a future specific agreement between the parties, regarding the processing of personal data, such a specific agreement should be negotiated and signed, as soon as possible. Concerning the hyper-scalers and/or their resellers, the relevant contract should be made complete in accordance with the provisions of the GDPR and specific to the processing of each case (not common in all cases independently of the characteristics of the processing).

**5. Difficulty regarding the freedom of choice of sub-processors**

**5.1. Short description:**

- Most public bodies seem to have no control over and cannot object meaningfully to the use of sub-processors or to changes of sub-processors at all or at least without risking a potentially critical loss of service.

- More specifically, the questionnaire respondents either provided no answer at all regarding sub-processors, or referred to the online list with the sub-processors of Microsoft[30]. This indicates that their knowledge is limited to the publicly available information by Microsoft and that they do not have control over the use of sub-processors, such as knowing exactly which one is involved in their particular usage of the cloud or having the chance to object to a specific sub-processor. Besides, the "Microsoft Cloud Services Sub-processors List" does not offer to the Controller a sufficient and clear overview of the sub-processors involved in its processing activities, since:

30 https://servicetrust.microsoft.com/ViewPage/TrustDocumentsV3?command=Download&downloadType=Document&downloadId=ede6342e-d641-4a9b-9162-7d66025003b0&tab=7f51cb60-3d6c-11e9-b2af-7bb9f5d2d913&docTab=7f51cb60-3d6c-11e9-b2af-7bb9f5d2d913_Subprocessor_List

- The above list does not contain adequate information on the location of data as it includes only the corporate location and not the exact location where the processing takes place.
- This list does not contain information of the chain of sub-processors.
- This list contains only reference to "customer data" and/or "pseudonymous data" without specifying the specific categories of personal data processed.

- In the case of the central buyer, public bodies don't have any control over the selection and use of sub-processors, because the central buyer chooses sub-processors through central governmental agreements (article 85 of law 4727/2020, article 28 par. 3 of law 4623/2019), while public bodies are legally bound to use the G-Cloud.

**5.2. <u>Which provisions of the GDPR this concerns:</u>**

- Articles 28(1), 28(2) GDPR

**5.3. <u>Why this has been an issue for the stakeholders:</u>**

- This deficiency makes it difficult for public bodies to comply with their obligation arising from Art. 28(1) GPDR, to "*use only processors providing sufficient guarantees" so* that the processing meets the requirements of the GDPR. The fact that public bodies have actually no control over the engagement of processor and sub-processors makes it difficult for them to ensure that the processing is compliant with the provisions of the GDPR, especially regarding transfers to third countries. Moreover, it is possible that, when a general authorization is provided, according to Art. 28(2) GDPR, the public body has no meaningful right to object, since the contract does not describe an efficient objection procedure (timeline, consequences etc.).

**5.4. <u>Differences between stakeholders:</u>**

- This issue seems to be common among public bodies as in all cases a hyper-scaler is involved (either directly as processor or indirectly as sub-processor of the central buyer). The public bodies do not have sufficient knowledge or control over the sub-processors involved in the processing or the extent of the processing except from general information made available by the hyper-scaler. A difference has been identified between the CSPs Microsoft and Oracle: While Microsoft does not provide enough information regarding the right to object to new sub-processors (the contract merely repeats the text of Art. 28 (2) GDPR), Oracle (Art. 4.3 of the "European DPA Addendum") describes a timeline (notification period) and foresees that in case of an objection "*Oracle and Customer will work together in good faith to find a solution to address such objection, including making the Services available without the involvement of such Third Party Sub-processor*".

**5.5. <u>Potential solutions to this issue by the SA or the stakeholders:</u>**

- The stakeholders should check with their CSPs to what extent and depth they can be informed about the specific sub-processors engaged in their processing activities, and under which provisions they can exercise their right to object according to Art. 28(2) GDPR.

**6. <u>Difficulty in determining technical and organisational measures to frame international transfers and access by foreign public authorities</u>**

**6.1. <u>Short description:</u>**

- Regarding international transfers, the questionnaire respondents provided answers by referring to the relative standard online texts of the hyper-scalers without specifying the details of transfers pertaining to their own data/systems.

- All questionnaire respondents declared that they have not received any access requests by USA Authorities.

- Regarding Microsoft, although Datacenters within the EU are used, respondents mentioned that, transfers of personal data, including telemetry/diagnostic data, to the US and third countries are based on the terms of the DPA and the information provided online for Office 365[31] and Azure[32] services. Microsoft collects pseudonymized data of the users managing the Azure infrastructure.

- Regarding Oracle, respondents mentioned that personal data (mostly financial data for tax purposes) are stored in the infrastructures of the central buyer within the country. The storage takes place in an automated manner on physical media (disks etc.) within the datacenters of the central buyer and the data is not transmitted outside of these datacenters by Oracle, either manually or automatically. Only systemic telemetry/diagnostic data is collected by the Oracle CSP, by default, through automated processes from the servers of the CSP. The telemetry/diagnostic data collected by Oracle is pseudonymized and limited to administrators' data.

- Detailed information on how the pseudonymization takes place from the CPS (Microsoft, Oracle) is not available and it is not clear whether appropriate safeguards are met.

- According to the section 'Data Transfers and Location' of the Microsoft DPA, "Taking into account such safeguards, Customer appoints Microsoft to transfer Customer Data, Professional Services Data, and Personal Data to the United States or any other country in which Microsoft or its Sub-processors operate and to store and process Customer Data, and Personal Data to provide the Products, except as described elsewhere in the DPA Terms". All transfers are governed by the 2021 Standard Contractual Clauses of the European Commission implemented by Microsoft. It is a processor to processors SCC signed between Microsoft Ireland Operations Limited and Microsoft Corporation.

- None of the questionnaire respondents has examined or negotiated supplementary technical and organizational measures. They only provide information to the measures that the CSP is capable to implement according to the available standard texts without specifying whether they have assessed the application of such measures. One questionnaire respondent mentioned that the negotiation of such supplementary measures is a long process, which would require to analyze, design and implement specific measures in its own environment and to amend the relevant legal texts.

**6.2. <u>Which provisions of the GDPR this concerns:</u>**

- Articles 44-47 GDPR

**6.3. <u>Why this has been an issue for the stakeholders:</u>**

- Unless the public bodies assess substantially whether specific technical and/or organizational measures should be applied, appropriate for their specific needs, they cannot efficiently limit personal data transfers in a way that is compliant with the provisions of Articles 44-47 GDPR: According to the Appendix C of the Microsoft DPA, "*In the event Microsoft receives an order from any third party for compelled disclosure of any personal data processed under this DPA, Microsoft shall: a. use every reasonable effort to redirect the third party to request data directly from*

[31] Office 365 - https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-dpia-office365

[32] https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-dpia-azure, https://azure.microsoft.com/mediahandler/files/resourcefiles/achieving-compliant-data-residency-and-security-with-azure/Enabling_Data_Residency_and_Data_Protection_in_Azure_Regions-2021.pdf

*Customer; b. promptly notify Customer, unless prohibited under the law applicable to the requesting third party, and, if prohibited from notifying Customer, use all lawful efforts to obtain the right to waive the prohibition in order to communicate as much information to Customer as soon as possible; and c. use all lawful efforts to challenge the order for disclosure on the basis of any legal deficiencies under the laws of the requesting party or any relevant conflicts with applicable law of the European Union or applicable Member State law*." But, according to Schrems II ruling (§185) "*the limitations on the protection of personal data arising from the domestic law of the United States on the access and use by US public authorities of such data transferred from the European Union to the United States, which the Commission assessed in the Privacy Shield Decision, are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required, under EU law, by the second sentence of Article 52(1) of the Charter*". Therefore transfers to the USA, without supplementary measures taken by the public bodies, as Controllers, may take place in breach of the GDPR and the Controllers may, consequently, not able to demonstrate compliance, according to the accountability principle.

**6.4. Differences between stakeholders:**

- Only one public body responded that no transfers of personal data take place, and, regarding telemetry/diagnostic data, especially in relation to Office 365, the telemetry feature is no longer provided by the CSP (Microsoft), therefore no transmission of such data takes place.

**6.5. Potential solutions to this issue by the SA or the stakeholders:**

- Controllers should assess and implement appropriate specific supplementary measures in order to frame possible transfers to third countries, based on their needs and processing characteristics. If such measures are not found sufficient, the public bodies should consider choosing another CSP. In case a breach is found, the SA may take action through corrective measures (orders or administrative fines).

## Part III – Actions by the SA

1. **Have you taken action (i.e. fact-finding exercises, informal contact, prior consultation, investigation) towards any of the stakeholders concerning the use of cloud-based services *prior to* launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

- Our SA has not taken any action towards any of the stakeholders prior to the coordinated action.

2. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (E.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**

- As this is an ongoing case, further investigation is required on the issues identified in the above analysis, particularly regarding the role of the parties involved in the processing and their obligations under the GDPR, the ability of the stakeholders to meaningfully negotiate with the CPS on the terms of the contract and the selection of the sub-contractors as well as the conditions under which international transfers take place.

- In this phase, the Authority plans to send letters to the parties involved in order to collect additional information, documentation and clarification with the goal to resolve the identified issues and publish recommendations and instructions to the public bodies.

- Then, based on the further results and evidence collected, the Authority will redefine its plan of action without excluding any corrective measures.

## Part IV – Other

1. **What is your general impression of the levels of awareness and compliance of the stakeholders you consulted concerning the use of cloud?**

- In general, the level of awareness can be considered as relative low at the beginning of the coordinated action. However, some public bodies reported that, in order to provide answers to the questionnaire, they started gathering information and considering issues that they had not examined thoroughly before. This already indicates an increase in the awareness level of public bodies, which the Authority intends to strengthen with its further actions.

2. **Are there any other issues or topics that you would like to flag?**

3. **Are there any leading practices of the stakeholders you have contacted that you would like to share?**

# ES SA

## AEPD National Report

### Part I - Statistics

1. **How many stakeholders have you contacted within the following categories?**

- 9 institutions Ministry of the central government
- 3 institutions Independent public body of the central government

2. **How many stakeholders have you contacted within the following sectors?**

- 1 institution: Agriculture
- 1 institution: Economic affairs
- 1 institution: Finance
- 1 institution: Health
- 2 institutions: Infrastructure
- 2 institutions: Justice
- 1 institution: Tax
- Other, 1 institution: Research
- Other, 1 institution: Culture
- Other, 1 institution: Governments coordinator

3. **If you have contacted a buyer, for which sectors does this buyer provides its services:**

- Not applicable.

4. **If you have contacted a buyer, and if you have this information, please specify the number of stakeholders this buyer provides services for:**

- Not applicable.

5. **What was the initial procedural framework of your action?**

- Fact-finding + determining follow-up action based on the results.

6. **How many stakeholders indicated that they use CSPs or are planning to do so in the near future (end of 2022)?**

- A total of twelve controllers were contacted. Eleven of them were already using CSPs and just one declares that has its own cloud infrastructure.

7. **Of the stakeholders that use CSPs (or are planning to do so in the near future), how many use CSPs for the following functions?**

- 11 institutions for Internal organisation (office suites, internal communication, HR, etc.).
- 7 institutions for Exercise of public functions (services to citizens, processing citizen's data, etc.).

8. **For the following commonly identified sectors, please specify if any hyper-scalers[33] are involved (if so please name them) either because they provide the services themselves or because the services are using the infrastructures of these hyper-scalers.**

- 1 institution – (Microsoft 365) - Finance
- 1 institution- (Amazon AWS) - Tax

[33] Hyper-scalers provide cloud services at scale. It refers usually to the big cloud providers (Google, AWS, Microsoft …) on which other services may also depend

9. **How many stakeholders took the following actions prior to- or during the acquisition of a CSP?**

- Perform a DPIA. **None.**
- Does the DPIA analyse transfers in detail (sometimes called DTIA). **None.**
- Contact the DPO for advice. **3 institutions.**
- Perform a general risk analysis. **None.**
- Contact the SA for advice. **None.**

10. **How many stakeholders (including buyers) take the following actions during the use of the CSP?**

- Monitoring technical and organisational measures to ensure compliance: **None**
- In case of transfers, adopting technical and organisational measures, including supplementary measures, where needed, and monitoring if changes in the regulatory landscape occur (e.g. Schrems II): **None of the institutions declares transfers of personal data.**
- Regular risk assessments: **None.**

## Part II - Substantive issues

1. **DPO involvement and position**

- Most of the controllers might have not consulted the DPO when they decided to hire the services of a CSP, which besides the lack of advice to data controller might involve difficulties with the position of the DPD.

- Provisions of articles 35 and 38. Although, in some cases, it is possible that the contractual terms had been achieved prior to the publication of the RGPD which, initially, would imply that these institutions, at that moment, had not designated the DPO given that in Spain the obligation to have a DPO materializes in 2016 with the publication of the RGPD.

- Most of the controllers explain that they did not consult the DPO when they decided to hire the services of a CSP since they understood that security measures were enough.
- On the other side, none of the controllers that have consulted the DPO did not received a negative response regarding the hiring of the CSP, which might also involve some misunderstanding on the side of the DPO as far as security as a principle of personal data protection and not as the only principle to consider.

**What are the differences that you have encountered between stakeholders in your Member State?**

- None. Most of the bodies did not consult the DPO.

**What are the solutions to this issue? Please describe if these solutions are already implemented or potential, and whether this solution is provided by the SA or the stakeholders.**

- Working on guidelines for data controllers and data processors within GDPR regulation, according to EDPB final report and recommendations, for instance, updating with these recommendations the Spanish guidelines for controllers and processors on the context of cloud computing.

2. **Risk Assessment**

- None of the entities has carried out a risk assessment when making this contract.
- Risk assessment for the rights and freedoms of citizens might have been understood as the risk assessment to set up security technical and organizational measures that would answer to GDPR article 32, which might mean a reduction of personal data protection to the mere existence of

security measures that could have been established without adequate assessment of risks referred to in recital 83, an issue that has been addressed in the guide to "Risk management and impact assessment in the processing of personal data of the AEPD".

- It seems that the reason might be a misunderstanding of the obligation to carry out a risk assessment according to the GDPR.

- None as none of the controllers has carried out a GDPR risk assessment.

**What are the solutions to this issue? Please describe if these solutions are already implemented or potential, and whether this solution is provided by the SA or the stakeholders.**

- Working on guidelines for data controllers and data processors within GDPR regulation, according to EDPB final report and recommendations, for instance, updating with these recommendations the Spanish guidelines for controllers and processors on the context of cloud computing.

**3. <u>Realization of DPIA</u>**

- In line with issue number 2, most of the controllers consulted have not carried out a DPIA of the services implemented in CSP.

- Article 35 of the GDPR. This should be an aspect included by CSP as a service by default characteristic at least within the context and scope they know.

- The fact that the CSP is certified according to the Spanish National Security Scheme was understood by most of the controllers and processors as more than enough for hiring the CSP services, so they did not consider carrying out a DPIA.
- Again, risk assessment for the rights and freedoms of citizens is reduced to providing security measures.

- There are no major differences, as most of the controllers consulted have not carried out a DPIA. One of the controllers has pointed out three CSP contracts in which the corresponding DPIA has been carried out but without doing the same in the rest of its contracts.
- Some of those who have not performed the DPIA do not respond to the reason why they do not perform the DPIA.

- Working on guidelines for data controllers and data processors within GDPR regulation, according to EDPB final report and recommendations, for instance, updating with these recommendations the Spanish guidelines for controllers and processors on the context of cloud computing.

**4. <u>D. Hiring the CSP and Contract Negotiation</u>**

- It seems that for some of the controllers the contract for hiring the CSP does not fully cover some key points of compliance with the GDPR, as it is the processor relationship.

- Article 28.3 states that the details of the processing by the processor shall be governed by a contract or other legal act and only a few bodies include this relationship in the contract.
- In the absence of a detailed analysis of this contractual relationship, it is unknown whether this is up to the so called "adhesion contracts" of the CSP service or whether the controller has the capacity to modify the contractual clauses to require the CSP to comply with the requirements of the GDPR.

- The main chosen CSP by almost all controllers is Microsoft with its Office 365 and Azure products. Followed by Amazon Web Services (AWS), which has been chosen by some entities.
- Regarding the obligations of the processor, only some bodies include them in the contract, and some bodies refer to the CSP being certified according to the Spanish National Security Scheme. Once again, GDPR and the obligations required by Article 28 might be reduced to the existence of a security framework regardless of the implicit risk that the processing could imply for the rights and freedoms of natural persons.
- Some of the controllers seem that they did not have any chance to negotiate the terms of the contract in order to reduce the possible risks related to the processing of personal data, which could reveal the existence of so-called "adhesion contracts" that come to be previously defined by the CSP without the possibility of modification by the data controller, though this cannot be determined from the scope of this report.

- The scope of the present action does not allow for a detailed analysis of the contracts between the institutions and the CSP, it is not possible to determine these differences.

- Besides working on guidelines for data controllers and data processors within GDPR regulation, according to EDPB final report and recommendations, for instance, updating with these recommendations the Spanish guidelines for controllers and processors on the context of cloud computing. We would suggest working based on the provisions of article 28 paragraphs 7 and 8 providing the market with contractual models according to GDPR provisions.

**5. <u>E. Audit and monitoring actions of controllers</u>**

- Monitoring of implementation of technical and organizational measures by the CSPs.

- It has only been identified monitoring of technical and organizational measures to ensure security of information and the continuity of the business operations of the institutions, that is, monitoring actions of CSPs in line with the certification procedures involved in each case. It is not known whether this is also the case when dealing with GDPR.

- As a verification measure, controllers generally verify that the CSP is certified according to the Spanish National Security Scheme.
- It is not known within the context of this report, whether controllers go beyond verifying security measures and do not verify other measures such as, for instance, data protection measures by design or by default, concrete application of the principle of minimization by the CSP or even security measures specifically aimed for managing rights and freedoms risks. A deeper and specific analysis based on each personal data processing should be required.

**What are differences that you have encountered between stakeholders in your Member State?**

- None of all the controllers monitors the implementation of technical and organizational measures.

**What are solutions to this issue? Please describe if these solutions are already implemented or potential, and whether this solution is provided by the SA or the stakeholders.**

- Once again, working on guidelines for data controllers and data processors within GDPR regulation, according to EDPB final report and recommendations, for instance, updating with these recommendations the Spanish guidelines for controllers and processors on the context of cloud computing.

## Part III - Actions by the SA

1. **Have you taken action (i.e. fact-finding exercises, informal contact, prior consultation, investigation) towards any of the controllers concerning the use of cloud-based services *prior to* launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the controller, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

- The AEPD did not take actions towards any of the questioned institutions prior to the coordinated action.

2. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (E.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing).**

- It is up to the general conclusions and recommendations of the final EDPB report.

## Part IV - Other

1. **What is your general impression of the levels of awareness and compliance of the stakeholders you consulted concerning the use of cloud?**

- It seems that there is not awareness at all about issues as data transfers, CSP processing telemetry data or foreign countries governments disclosing the data.

2. **Are there any other issues or topics that you would like to flag?**

- No

3. **Are there any leading practices of the stakeholders you have contacted that you would like to share?**

- One of the consulted controllers have declared that for security reasons they have established in their internal regulations the strict control of all sensitive information, both from the point of view of personal data protection and information security, and according to this they do not use any CSP. For its own business operation, this controller has its own private cloud, managed by itself and without hiring any external service.

# FI SA

## The Office of the Data Protection Ombudsman

### Part I – Statistics

1. **<u>How many stakeholders have you contacted within the following categories?</u>**

- Ministry of the central government
- Independent public body of the central government: **2 stakeholders**
- Buyer for the central government: **1 stakeholder**
- Publicly-owned company acting as a processor for several central public bodies
- Ministry of the regional government
- Independent public body of the regional government
- Buyer for the regional government
- Publicly-owned company acting as a processor for several regional public bodies
- Other, please specify

2. **<u>How many stakeholders have you contacted within the following sectors?</u>**

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government: **1 stakeholder**
- Economic affairs
- Education
- Finance
- Health
- Infrastructure
- Employment
- Justice
- Tax: **1 stakeholder**
- Other, please specify: **Government ICT centre - 1 stakeholder**

3. **<u>If you have contacted a buyer, for which sectors does this buyer provides its services:</u>**

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government
- Economic affairs
- Education
- Finance
- Health
- Infrastructure
- Employment
- Justice
- Tax
- No specific sector: **1 stakeholder - All government agencies and institutions, also including government-owned corporations, other public authorities, bodies governed by public law, the parliament, funds that are not within the scope of the government budget and companies or organisations with public administration or service responsibilities.**
- Other, please specify

4. **<u>If you have contacted a buyer, and if you have this information, please specify the number of stakeholders this buyer provides services for:</u>**

- This information was not requested from the stakeholders the FI SA contacted.

5. **<u>What was the initial procedural framework of your action?</u>**

– Fact finding
– **Fact finding + determining follow-up action based on the results**
– New investigation[34]
– Ongoing investigation

6. **<u>How many stakeholders indicated that they use CSPs or are planning to do so in the near future (end of 2022)?</u>**

- All 3 stakeholders

7. **<u>Of the stakeholders that use CSPs (or are planning to do so in the near future), how many use CSPs for the following functions?</u>**

- Internal organisation (office suites, internal communication, HR, etc.): **all 3 stakeholders**
- Exercise of public functions (services to citizens, processing citizen's data, etc.): **all 3 stakeholders**

8. **<u>For the following commonly identified sectors, please specify if any hyper-scalers[35] are involved (if so please name them) either because they provide the services themselves or because the services are using the infrastructures of these hyper-scalers.</u>**

– Health
– Finance
– Tax – **Microsoft**
– Education
– Central buyers or providers of IT services - **AWS, Microsoft**

9. **<u>How many stakeholders took the following actions prior to- or during the acquisition of a CSP?</u>**

– Perform a DPIA: **2 stakeholders**
– Does the DPIA analyse transfers in details (sometimes called DTIA): **2 stakeholders**
– Contact the DPO for advice: **all 3 stakeholders**
– Perform a general risk analysis: **all 3 stakeholders**
– Contact the SA for advice

10. **<u>How many stakeholders (including buyers) take the following actions during the use of the CSP?</u>**

– Monitoring technical and organisational measures to ensure compliance: **all 3 stakeholders**
– In case of transfers, adopting technical and organisational measures, including supplementary measures, where needed, and monitoring if changes in the regulatory landscape occur (e.g., Schrems II): **2 stakeholders**
– Regular risk assessments: **all 3 stakeholders**

## Part II – Substantive issues

[34] making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred

[35] Hyper-scalers provide cloud services at scale. It refers usually to the big cloud providers (Google, AWS, Microsoft …) on which other services may also depend

1. **At pre-contractual phase**

**1.1. Other stakeholders (controllers) cannot effectively affect the decisions made by the central buyer regarding the use of CSPs (incl. transfers to third countries)**

- Relates to Articles 24, 28, 44 and 46 GDPR.
- One stakeholder stated that it cannot fully ensure the lawfulness of the processing performed by the sub-processors. This stakeholder has also stated that they only have limited knowledge regarding the sub-processors used by the CSP. The contract between the other stakeholders (customers) and the central buyer states that personal data may only be accessed and processed within the EEA unless there is a prior written consent of the controller. Regardless of this, the central buyer seems to use sub-processors that transfer personal data to third countries. It should be noted, that for the stakeholders the use of the central buyer is mandatory under Finnish legislation.
- The controller should have power regarding the use of sub-processors as described in Article 28 GDPR and the central buyer should only use sub-processors which process data within the EEA unless otherwise agreed upon.
- There have been some inaccuracies in the contract between the central buyer and Microsoft regarding roles. In 2021, the central buyer added an additional agreement to the contract with Microsoft where it was clarified that other stakeholders act as controllers. This additional agreement mainly clarifies the roles between the central buyer and the stakeholders (its customers).

2. **In the contract with the CSP**

**2.1. CSPs are processing personal data for their own purposes**

- Relates to Articles 28(1) and 28(10) GDPR.
- Stakeholders cannot ensure compliance with the GDPR since they cannot change the CSP even if the (sub-) processor would process personal data against the GDPR and/or the stakeholder's instructions.

**2.2. Stakeholders have restricted negotiating power in relation to contracts with the CSPs**

- Relates to Articles 28(1), 28(3) and 28(10) GDPR
- The contract between stakeholders and AWS/Microsoft is mainly predetermined by AWS/Microsoft.

**2.3. Stakeholders have no influence on the sub-processors used by AWS/Microsoft. Not all the sub-processors have been identified.**

- Relates to Article 28(2) GDPR.
- The central buyer has stated that AWS/Microsoft informs its customers about changes made to the sub-processors in its newsletter/on its website. The central buyer can object to the use of such sub-processors only by terminating the contract.

3. **On International transfers and access by foreign public authorities**

**3.1. No transfer impact assessment (TIA) has been made regarding the use of CSPs**

- Relates to Articles 24, 44 and 46 GDPR.
- One stakeholder has performed its own TIA relating to Microsoft and at the time of the survey, this stakeholder was working on its own TIA relating to AWS. Another stakeholder has not performed a TIA since it is of the opinion that there are no data transfers outside the EU/EEA.

**3.2. Stakeholders have not been able to identify appropriate and effective supplementary measures.**

- Relates to Articles 44 and 46 GDPR.

- This matter has been an issue for all three stakeholders because there are no appropriate safeguards to ensure the required level of protection when transferring personal data to third countries. It seems that the central buyer has not been able to process personal data in accordance with all of the controller's (customer's) instructions.
- One stakeholder has identified technical supplementary measures in most cases (encryption, pseudonymization, Customer Lockbox) but their effectiveness is not always clear (e.g., in some cases the encryption keys are governed by the CSP and device and user data is possibly transferred to the U.S.). The stakeholder in question states that the risk for data subjects has been estimated to be low, as the transferred information is restricted and includes employee names and emails, which are nationally regarded as public information. However, the supplementary measures that two of the stakeholders have adopted seem inadequate and e.g., in relation to support and maintenance tasks no supplementary measures have been identified.

**3.3. Risk of access by foreign public authorities**

- Relates to Article 6 and Chapter V GDPR.
- One stakeholder has identified that foreign public authorities could have access to the personal data under third country legislation. However, the stakeholders have not been notified of any request for disclosure of personal data. Another stakeholder thinks it is unlikely that public authorities in the U.S. would try getting access to the data via intelligence gathering, as there are many international agreements related to the information it processes that already offer the U.S. authorities the possibility to get access to relevant information in a more efficient way.

## Part III – Actions by the SA

1. **Have you taken action (i.e., fact finding exercises, informal contact, prior consultation, investigation) towards any of the stakeholders concerning the use of cloud based services *prior to* launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g., letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

- No.

2. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (e.g., letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**

- The FI SA has not yet decided what actions will be taken in this matter. The investigation is still ongoing.

- However, the FI SA stresses that in the Schrems II judgment (C-311/18), the Court clearly stated that if a supervisory authority takes the view, following an investigation, that a data subject whose personal data have been transferred to a third country is not afforded an adequate level of protection in that country, it is required, under EU law, to take appropriate action in order to remedy any findings of inadequacy, irrespective of the reason for, or nature of, that inadequacy. Therefore, if the FI SA takes the view that stakeholders have infringed Chapter V of the GDPR, the FI SA must use its corrective powers listed in Article 58(2) of the GDPR.

- It should be noted that an administrative fine cannot be issued to public authorities in Finland.

## Part IV – Other

1. **What is your general impression of the levels of awareness and compliance of the stakeholders you consulted concerning the use of cloud?**

- The general level of awareness related to the data protection issues when using CSPs seems satisfactory, but several concerns remain.

- The first stakeholder is aware of the risks concerning the use of CSPs. It has stated that there is a conflict, which arises from the fact that the contract terms of CSPs do not meet the requirements of the GDPR in all respects. The second stakeholder has taken many measures (risk assessments, DPIA, TIA, cooperation and information sharing with stakeholders and international colleagues) in trying to ensure its compliance with the GDPR and Chapter V. However, several issues remain as described above. The third stakeholder points out that it has little power in ensuring GDPR compliance due to the central buyer being responsible for the acquisition of CSPs. This stakeholder emphasizes its contract with the central buyer and the responsibilities of the central buyer as a processor and the fact that according to their agreement personal data should only be processed and accessed within the EEA, unless prior written consent is given by the stakeholder.

- Stakeholders also refer to the constantly changing legal environment, partly contradictory case law in different Member States and lack of guidance from SAs as further challenges.

2. **Are there any other issues or topics that you would like to flag?**

3. **Are there any leading practices of the stakeholders you have contacted that you would like to share?**

# IS SA

## Icelandic Supervisory Authority - Persónuvernd

### Part I – Statistics

1. **How many stakeholders have you contacted within the following categories?**

- Ministry of the central government: **None**
- Independent public body of the central government: **None**
- Buyer for the central government: **None**
- Publicly-owned company acting as a processor for several central public bodies: **None**
- Ministry of the regional government: **None**
- Independent public body of the regional government: **None**
- Buyer for the regional government: **Six municipalities**
- Publicly-owned company acting as a processor for several regional public bodies: **None**
- Other, please specify: **Not relevant**

2. **How many stakeholders have you contacted within the following sectors?**

- Agriculture: **None**
- Defence: **None**
- Digitalisation of the Public Administration/e-Government: **None**
- Economic affairs: **None**
- Education: **Six**
- Finance: **None**
- Health: **None**
- Infrastructure: **None**
- Employment: **None**
- Justice: **None**
- Tax: **None**
- Other, please specify: **Not relevant**

3. **If you have contacted a buyer, for which sectors does this buyer provides its services:**

- Education

4. **If you have contacted a buyer, and if you have this information, please specify the number of stakeholders this buyer provides services for:**

- Municipality of Akureyri: 10 elementary schools
- Municipality of Garðabær: 6 elementary schools
- Municipality of Hafnarfjörður: 9 elementary schools
- Municipality of Kópavogur: 9 elementary schools
- Municipality of Reykjanesbær: 7 elementary schools
- Municipality of Reykjavík: 39 elementary schools

5. **What was the initial procedural framework of your action?**

- New investigation in the form of audits.

6. **How many stakeholders indicated that they use CSPs or are planning to do so in the near future (end of 2022)?**

- All six. However, the scope of the investigation has been limited to the use of cloud services provided by Google LLC, and additionally in the case the municipality of Kópavogur, Seesaw, for

the processing of personal data regarding students at elementary schools (age 6-16). However, the DPA's investigation of the municipality of Akureyri has been terminated, as it was not found to be a controller, under article 4(7) of Regulation (EU) 2016/679 of the data processing subject to the scope of the investigation. This was due to the fact that the municipality does not decide whether its elementary schools are to use CSPs, and if so, which ones. Rather individual elementary schools, operated by the municipality, decide individually whether they introduce cloud-based services in their teachings and which CSPs are appropriate for that purpose.[36]

**7. <u>Of the stakeholders that use CSPs (or are planning to do so in the near future), how many use CSPs for the following functions?</u>**

- Internal organisation (office suites, internal communication, HR, etc.): **Not relevant in the light of the scope of the investigation, as discussed under question 6.**
- Exercise of public functions (services to citizens, processing citizen's data, etc.): **Five**

**8. <u>For the following commonly identified sectors, please specify if any hyper-scalers[37] are involved (if so please name them) either because they provide the services themselves or because the services are using the infrastructures of these hyper-scalers</u>**

- Education / Google LLC

**9. <u>How many stakeholders took the following actions prior to- or during the acquisition of a CSP?</u>**

- **Perform a DPIA:**

  **In relation to services provided by Google:**

  - DPIAs in relation to the use of Google's cloud-based services have been presented by three municipalities. However, two municipalities are of the view that they were not obliged to perform DPIAs in relation to Google services as their use was initiated before the Icelandic Data Protection Act no. 90/2018 (which incorporates Regulation (EU) 2016/679 to Icelandic Law) came into force. Yet, both municipalities have informed the SA that DPIAs are currently being performed in relation to the services.

  **In relation to services provided by Seesaw:**

  - DPIA in relation to the use of Seesaw's cloud-based services has been presented by the only municipality that is under investigation for the use of the CSP.

- **Does the DPIA analyse transfers in details (sometimes called DTIA):**

  **In relation to services provided by Google:**

  - DPIAs of two municipalities contain provisions, to a varying degree of detail, on transfer of personal data to third countries.

  **In relation to services provided by Seesaw:**

  - DPIA contains a general provision on the transfer of personal data to the United States.

[36] The SA takes notice of this scope when providing answers to following questions in this report. As a result, the replies below reflect only the actions and inactions of the municipalities that are currently under investigation by the SA in relation to their use of services of Google and Seesaw in the field of education. In contrast, information related to the use of *other* CSPs by the municipalities that are under investigation are disregarded. Similarly, information regarding the use of all CSPs by the municipality of Akureyri are disregarded.

[37] Hyper-scalers provide cloud services at scale. It refers usually to the big cloud providers (Google, AWS, Microsoft …) on which other services may also depend

- **Contact the DPO for advice**

  **In relation to services provided by Google:**

  - It appears that DPOs have been contacted for advice to some degree by four to five municipalities (uncertainty in the light of the discussion under the next bullet) in relation to their use of cloud-based services provided by Google, either prior, during or after the introduction of the services. However, it must be noted that some of the municipalities did not employ DPOs when the use of the services was initiated.

  **In relation to services provided by Seesaw:**

  - It appears that the DPO was not contacted in relation to the introduction of the service in question. However, in the replies of the municipality that are not software-specific, it holds that the DPO is contacted in later stages in the relation to introduction of cloud-based services in general, e.g. for review of DPIOs and risk assessments. Yet, the municipality has admitted that the DPO's advice to seize the use of Seesaw, given after the SA's decision discussed under part III, was not adhered.

- **Perform a general risk analysis**

  All five municipalities appear to perform a general risk analysis to some degree in relation to cloud-based services. It should also be highlighted that the Icelandic Association of Local Authorities has performed a general risk analysis for multiple software programs in the field of education.

- **Contact the SA for advice**

  A survey of the SA's case registry indicates that two of the municipalities, that are under the current investigation, made a joint request for an information meeting with the authority, regarding the use of CSPs, including cloud-based services provided by Google in the field of education. The request was granted by the authority. According to the meeting minutes, the municipalities were provided with some general information on the matter.

**10. <u>How many stakeholders (including buyers) take the following actions during the use of the CSP?</u>**

- Monitoring technical and organisational measures to ensure compliance: **Two municipalities monitor, to some degree, technical and organisational measures to ensure compliance. Three municipalities do not monitor technical and organisational measures to ensure compliance.**
- In case of transfers, adopting technical and organisational measures, including supplementary measures, where needed, and monitoring if changes in the regulatory landscape occur (e.g. Schrems II): **One municipality has adopted technical and organisational measures, including supplementary measures, where needed, in the case of transfers. Four municipalities do not appear to have adopted such measures. None of the municipalities monitor changes in the regulatory landscape in a systematic manner, although four of them perform checks if need arises (incident-based approach).**
- Regular risk assessments: **None of the municipalities appears to perform systematic risk assessment.**

## Part III – Actions by the SA

**1. <u>Have you taken action (i.e. fact-finding exercises, informal contact, prior consultation, investigation) towards any of the stakeholders concerning the use of cloud-based services *prior to* launching the coordinated action? Please describe the action you have taken and the</u>**

**outcome of this action (e.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

- In April 2021, the Icelandic Supervisory Authority (SA) was notified that one of Reykjavík's elementary schools was obtaining consent from parents for processing of personal data of students using the Seesaw educational system, which is an American cloud-based service. The Icelandic SA subsequently examined on its own initiative the use of the Seesaw educational system by elementary schools in Reykjavík.

- On December 20, 2021, the Icelandic SA concluded that the municipality of Reykjavík had breached various provisions of the GDPR using Seesaw. Following that decision, the Icelandic SA examined whether there were grounds for imposing an administrative fine. In its decision on May 3, the Icelandic SA concluded that the municipality of Reykjavík was to pay a 5.000.000 ISK fine.

- Key findings of the Icelandic SA's former decision were i.a. that the processing agreement between Reykjavík and Seesaw was insufficient, that the municipality could not demonstrate a specified, explicit and legitimate purpose for the processing in question, which was therefore considered unlawful, that the processing was neither fair nor transparent, that the principles of data minimisation and storage limitations were not implemented nor data protection by design and by default, taking into consideration the amount of data collected, the extent of their processing, the period of their storage and their accessibility, that the data protection impact assessment did not meet the minimum requirements, that the municipality did not demonstrate that it had ensured appropriate security of the personal data in question and that the data was being transferred to the United States without appropriate safeguards.

- The Icelandic SA furthermore concluded that all processing in the Seesaw educational system should be seized and students' data deleted after being retrieved, if applicable, to be stored within each school.

- Key findings of the latter decision were that, due to all the above and taking into consideration i.a. that the infringements concerned the personal data of children and that it was considered likely that special categories of data and other sensitive information were being processed; but also that no damage appeared to have been caused by the violations, that there was no indication that Seesaw's general information security was not adequate and that the municipality co-operated with the SA in a clear and concise manner, a 5.000.000 ISK administrative fine was imposed on the municipality of Reykjavík.

- The SA's decision was to impose an administrative fine on Reykjavik of a fee of appr. 35.768 EUR.

**2. What action(s) are you planning to undertake based on the results of this coordinated action, if any? (E.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**

- The Icelandic SA has not determined the appropriate course of actions based on the coordinated enforcement actions, given the fact that no decision on the legality of substantive issues has been rendered. In this context, it must also be stressed that according to article 38(3) of the Icelandic Data Protection Act no. 90/2018, the SA's board is responsible for making any major material or policy-making decisions in matters that are being processed by the authority, including the imposition of administrative fines.

## Part IV – Other

1. **What is your general impression of the levels of awareness and compliance of the stakeholders you consulted concerning the use of cloud?**

- The SA is of the view that all five municipalities, currently under investigation, have a rudimental awareness regarding the use of cloud-based services and data protection. However, in the light of the discussion under question 2 in part III, the SA does not view it as timely to signal its impression on the municipalities' compliance to the legal framework of data protection.

2. **Are there any leading practices of the stakeholders you have contacted that you would like to share?**

- Not relevant.

# IT SA

## Italian SA – Garante per la protezione dei dati personali

### Part I – Statistics

1. **How many stakeholders have you contacted within the following categories?**

- Ministry of the central government: **1**
- Independent public body of the central government
- Buyer for the central government
- Publicly-owned company acting as a processor for several central public bodies: **2**
- Ministry of the regional government
- Independent public body of the regional government
- Buyer for the regional government
- Publicly-owned company acting as a processor for several regional public bodies: **2**
- Other, please specify

2. **How many stakeholders have you contacted within the following sectors?**

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government: **X**
- Economic affairs
- Education
- Finance
- Health
- Infrastructure
- Employment
- Justice
- Tax
- Other, please specify: **By addressing our action to publicly-owned companies acting as processors for several public bodies (at both national and regional level), many stakeholders in different sectors of the public administration could be involved (indirectly) including the sectors of Digitalisation of public administration, Finance, Health and Social security, Tax, Infrastructures, Employment, Justice.**

3. **If you have contacted a buyer, for which sectors does this buyer provides its services:**

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government
- Economic affairs
- Education
- Finance
- Health
- Infrastructure
- Employment
- Justice
- Tax
- No specific sector
- Other, please specify: **N/A**

4. **<u>If you have contacted a buyer, and if you have this information, please specify the number of stakeholders this buyer provides services for:</u>**

- N/A

5. **<u>5What was the initial procedural framework of your action?</u>**

- Fact finding
- Fact finding + determining follow-up action based on the results: **X**
- New investigation[38]: **X**
- Ongoing investigation: **X**

6. **<u>How many stakeholders indicated that they use CSPs or are planning to do so in the near future (end of 2022)?</u>**

- All stakeholders are using or planning to use CSPs by the end of 2022 for some services

7. **<u>Of the stakeholders that use CSPs (or are planning to do so in the near future), how many use CSPs for the following functions?</u>**

- Internal organisation (office suites, internal communication, HR, etc.): **All of them use (different) cloud services for their internal organisation**
- Exercise of public functions (services to citizens, processing citizen's data, etc.): **All of them use CSPs (and plan to use them) for the exercise of public functions**

8. **<u>For the following commonly identified sectors, please specify if any hyper-scalers[39] are involved (if so please name them) either because they provide the services themselves or because the services are using the infrastructures of these hyper-scalers</u>**

- Health
- Finance
- Tax
- Education
- Central buyers or providers of IT services
- In most cases, the main hyper-scalers are involved both because they provide the services and because their infrastructures are used

9. **<u>How many stakeholders took the following actions prior to- or during the acquisition of a CSP?</u>**

- Perform a DPIA: **2**
- Does the DPIA analyse transfers in details (sometimes called DTIA): **1**
- Contact the DPO for advice: **2**
- Perform a general risk analysis: **1**
- Contact the SA for advice: **1**

10. **<u>How many stakeholders (including buyers) take the following actions during the use of the CSP?</u>**

- Monitoring technical and organisational measures to ensure compliance: **3**
- In case of transfers, adopting technical and organisational measures, including supplementary measures, where needed, and monitoring if changes in the regulatory landscape occur (e.g. Schrems II): **0**

[38] making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred

[39] Hyper-scalers provide cloud services at scale. It refers usually to the big cloud providers (Google, AWS, Microsoft …) on which other services may also depend

– Regular risk assessments: **2**

## Part II – Substantive issues

**1. <u>At pre-contractual phase</u>**

**1.1. <u>Role of the resellers from a data protection point of view and responsibilities in case of inconsistency between the public procurement and the contract signed with the CSP.</u>**

- One of the main issues identified in relation to the pre-contractual phase is related to the role of the resellers of cloud services. Usually, the cloud services are not directly negotiated with the CSPs (in many cases hyper-scalers) but via Italian companies acting as resellers and the exact role of these resellers is not always clear from a data protection point of view. In some cases, for example, even where the resellers do not play any active role in processing personal data in relation to the provision of the cloud services, they have been nevertheless designated as data processors.

- GDPR provision concerned: Article 28 and, in particular, the way in which obligations under art. 28(3) GDPR may be complied with in practice.

- This issue has been dealt with in different ways. In some cases, resellers are considered to be solution providers that play only an intermediation role for the purchase and payment of services, while, with regard to the processing of personal data, the hyper-scaler has a direct relationship with the public body (which includes the public authority as the controller and the publicly-owned company acting as processor for a given public authority, all of them being referred to hereinafter as 'PA') which has designated the CSP as data processor/sub-processor (so called "End Customer Account Model"). This model provides for a direct relationship between the PA and the hyper-scaler for the access to and use of cloud services, thus ensuring – among the other things – the continuity of the services even following termination of the contract with the reseller.

- In other cases, the relationship between the PA and the hyper-scalers is mediated by the resellers, which are designated as data processors even though they do not process personal data in relation to the cloud services provided. The Data Processing Agreement/Addendum is undersigned between the reseller and the CSP, and the PA has no direct relationship with the CSP. Indeed, on the assumption of the absence of a direct contractual relationship between the PA and the CSP, CSPs require the PA to interact with the reseller and commit all compliance obligations to the reseller, whilst in practice all services and processing activities are carried out directly by the CSPs. In these cases, it is difficult for the PA to provide full instructions to the actual processor and to assess its compliance: CSPs often refuse to accept to negotiate specific clauses in the contracts with the PA and to receive direct instructions from them. These difficulties seem to be compounded by the widespread use of model contracts in which it is clearly stated that they are to be considered as Customer's documented instructions for the processing of Personal Data and which may only be adhered to without any possibility to negotiate specific amendments (see issues related to difficult negotiations).

- In addition, some stakeholders have complained that there are cases where they have provided the reseller acting as a processor with specific instructions (e.g. to provide information on data breaches within a specific timeframe), but the same instructions have not been imposed on the CSPs because of the reduced ability to negotiate clauses that, as mentioned before, are already contained in the contract/data processing addendum prepared by the CSP.

**2. <u>In the contract with the CSP</u>**

### 2.1. Difficult negotiations and unilateral amendments

- In all investigated cases, it was difficult for the public administration to negotiate a bespoke contract, considering that hyper-scalers offers standard contracts they may unilaterally modify.
- GDPR provision concerned: Article 5(2) and Article 28 GDPR.

- Stakeholders generally complained about the main difficulties encountered in this context and in particular called the attention to: 1. the difficulties for the PA to negotiate aspects relating to the protection of personal data processed by the CSP on its behalf, pending the reseller's intermediation in the aforementioned contractual relationship (see previous issue relating to the resellers' role) and considering that the resale contract is not different from the contract for the provision of the service; 2. The imbalance in negotiation with the main CSPs on the market, which make use of predefined service terms, in relation to which the PA has often not been able to obtain all the changes required; 3. How service terms are amended and how they are notified. The notification rules are the same for any kind of contractual amendment; however, according to the stakeholders, these rules should be different (e.g. in the timing envisaged) by having regard to the different characteristics and impact of the amendments on the processing of personal data.

- It is a widespread impression among the stakeholders that when various public bodies try to cooperate in negotiating with the CSPs or if one of them negotiates the same services on behalf of several public bodies, the imbalance in negotiation seems to be reduced and this is the reason why few of them already tried in the past to have talks with other entities at national level (including when possible the central buyers) at least in order to identify and discuss the main criticalities of the contracts for the services provided by the main CSPs and possible ways of addressing them. However, in the absence of coordinated actions, each PA has to independently negotiate conditions or settings with the CSP and this undermines their power.

- In a few cases, the stakeholders have initiated talks with the CSP aimed at negotiating some changes to the current standard contract in place. These discussions have made it possible to clarify certain aspects of contractual clauses contained in the DPA, but have not led generally to the negotiation of specific conditions with some minimal exceptions. However, following some requests for clarification or modification made by the stakeholders, the CSP has amended its standard documentation.

### 2.2. Designation of sub-processors

- Usually, the CSPs engage sub-processors on the basis of general written authorisations by the PA which are given the opportunity to object to any change to the list. However, PA are often informed about the sub-processors involved in routine service provision or support services by means of webpages in which they are listed and only in some cases (e.g. if the public authorities have indicated contact details, such as an email address) are they informed directly about amendments to such list and therefore about changes of sub-processors. In most cases, failure to object to new sub-processors is interpreted as an authorisation and if the PA objects to a sub-processor, the usual contractual recourse is to terminate its subscription to the given service. If the service is part of a suite, the PA must terminate its subscription to the entire suite. The other option, especially for sub-processors providing support services, is to limit as far as possible both the use of the service in question and the data shared in connection with a support case. All of this could result in the loss of potentially business critical services and have implications for the controller's ability to deliver public services in a timely manner and, as a result, risks undermining the right to object to changes of sub-processors envisaged by Article 28(2) GDPR in case of a general authorisation.

- GDPR provision concerned: Article 28 (2) and 28(4).

- Difficulties have been highlighted by PA in negotiating different rules on the identification/changes of sub-processors since most CSPs seem not to be inclined to change their model considering that, in many cases, it would not be possible for them to provide services in a different way.

- Furthermore, generally, there is no specific list of the sub-processors that are actually used by the CSP to provide the required services to the relevant PA. The list provided is a general one and, even in the course of or after the investigations, it was difficult for the PA to be provided with information about the sub-processor involved in the processing activities related to the services provided to them - in spite of the need for the controller to be in effective control of the chain of entities processing personal data on its behalf. Only in a few cases, upon specific request, has the public authority been provided with the list of the specific sub-processors.

- Reference should be made to a case where, in order to try to ensure that the controller retained a sufficient level of control over the selection of new sub-processors, a contractual amendment was implemented so as to grant the controller a meaningful right to review the change of the list of relevant sub-processors and to transmit reasoned objections within a predefined period. In this event, the CSP may obtain the termination of the contractual relationship only if the CSP is unable to provide the services without the use of the sub-processor objected to. This model could be of help especially where provisions are included in the contract defining criteria for the selection of new sub-processors and providing that such criteria must be met if the controller's failure to object within a given deadline is to be interpreted as an authorisation.[40]

### 2.3. Processing activities of the CSP for its business purposes

- CSPs process some personal data in order to provide cloud services to PA and, in some cases, for their own business purposes. However, following the investigation activities, it appears that national stakeholders are not fully aware of the categories of personal data collected in this respect and the specific purposes for which they are processed - mainly because of the very high-level wording usually included in the CSP's model contracts.

- GDPR provision concerned: Articles 5, 6, 9 and 28 (28.3 and 28.10 in particular).

- In particular, for SaaS services, some CSPs' standard contracts envisage that the CSP could act as a data "controller" in relation to the processing of personal data in connection with its business operations. In these cases, it appears that the data protection regimes applicable to personal data collected and processed by CSPs for their own purposes may be other than those envisaged for the personal data processed on behalf of the PA (i.e., the CSPs usually apply the data protection rules they are subject to in respect of the personal data they process for providing the cloud services and for the business operations rather than the specific safeguards included in the Data Processing Agreements/Addendums signed with the PA).

- Upon specific requests, in some cases, CSPs provided the PA with additional information in this regard (e.g., in one case, it was explained that they considered all personal information collected or generated during the provision and administration of their cloud services as 'service data' they processed as a controller, including any "diagnostic data" related to how those services are used).

[40] EDPB, *Guidelines 07/2020*, paragraph 157, p. 43.

- Unclear information about the categories of personal data collected/generated from users of cloud services and the business purposes for which such data are processed raises concerns in relation to the appropriate legal basis for such kind of processing carried out by the CSPs as well as regarding compliance with the different obligations and responsibilities applying to controllers and processors in relation to the cloud services provided. From this perspective, a further assessment exercise should be carried out taking into account that, according to Article 28(3) GDPR, processors should process personal data only on documented instructions from the controller unless required to do so by Union or Member State law to which the processor is subject. This is all the more important for cases where 'service data' could be related to users other than the PA employees, i.e. to the individuals to whom public services are provided by the public authority (e.g., public Wi-Fi users, students using e-learning platforms, etc.).

- In this context, a few contractual changes have been negotiated in a specific case, on the PA's request, aimed at limiting the processing of personal data by the CSP for its own purposes.
- This issue seems to have a more limited impact when cloud services are deployed as PaaS or IaaS considering that the amount of personal data 'generated' from the use of these services is far less substantial than the one 'generated' when SaaS are involved.

## 3. On International transfers and access by foreign public authorities

### 3.1. Transfer awareness and instructions on transfers

- In relation to transfer awareness, the circumstance that the European region is specified in most cases as the place for the processing of personal data by CSPs would appear to give a wrong impression that no transfers are taking place. Only after the investigation activities and some specific questions related to provisions included in the Data Processing Agreements/Addendums referring to possible transfers, did some public authorities realize that data at rest is usually stored in the selected region, however there could be cases where the CSP cannot provide a service from the selected region as it needs to transfer data to third countries (e.g. typically in the case of 'round the clock' services); accordingly, the only way to avoid the transfers of personal data would be by refraining from use of the service at issue. Furthermore, this is usually the case with the processing of personal data for the CSPs' own business purposes (see previous point).

- In some cases, a list of the services that cannot be provided without transferring personal data to third countries is provided to the PA; in other cases, the situation concerning transfers is less clear as they may depend on the possible use of individual services provided by sub-processors established in third countries, which are only referred to in bulk in the list of (possible) sub-processors (see previous point n. 4 on the difficulties in identifying the actual sub-processors involved in the processing of personal data on behalf of each relevant PA and consequences on the fulfilment of Article 30 GDPR – see point 9).
- GDPR provisions concerned: Article 5(1)a and 5(2), 28(3)a and Chapter V.

- In order to frame these possible transfers, it is usual for Data Processing Agreements/Addendums, as unilaterally drafted by the CSPs, to refer to SCCs as the tool to be used 'in case' of transfers. However, those SCCs are not accompanied by specific Annexes describing the specific (possible) transfers at issue. Annexes to the SCCs attached to the CSPs' model contracts signed by the PA are always the same and do not contain any specific description of the (possible) flows of personal data in relation to the cloud services provided to the relevant PA; in fact, the wording in the Annexes is the same as the (general) one contained in the CSPs' model contracts. For example, some annexes of SCCs for processor-to-processor transfers attached to the CSPs' model contracts refer to the competence vested in the Supervisory Authority of the EEA processor, while it should

be clear that the competent Supervisory Authority to be referred to is the one competent for (each) relevant PA in case of processing activities carried out on behalf of PAs.

- While one could argue that that this model depends on the need to frame services provided worldwide by the CSPs to thousands of controllers, on the other hand, merely attaching the SCCs to the model contracts without any clear indication of the possible flows of data that they may cover risks undermining the controller's role and responsibilities in case of transfers pursuant to Article 28(3)a GDPR.

- Furthermore, mainly because of the lack of awareness about the possible existence of data transfers, generally, no transfer impact assessment is carried out by the PA and, even when it is carried out, it does not always cover all possible data transfers and third countries involved. In this respect, some stakeholders complained that it would be very difficult to assess the legislation of all third countries where possible processors may be established, especially where there is a lack of information about the sub-processors that are actually involved in the services provided to the PA. The lack of awareness on data transfers and the subsequent failure to assess the third countries involved in the possible transfers also impact the need to assess if the obligations set forth in the specific transfer tools can be complied with by the CSPs where the legislation of the third country may impinge on those obligations. After the Schrems II case, CSPs integrated their model contracts by Addendums referring to some additional measures in relation to the obligations to carry out an assessment of the legislation of the third country to which data are transferred and to adopt supplementary measures, where necessary, so as to ensure that the level of protection afforded by the GDPR would not be undermined once data are transferred. However, as clarified in the Recommendation 1/2020 on supplementary measures, there could be cases where the processor retains access to data in the clear following transfers or needs to access data in the clear in at least some cases, for example when scanning for security threats and, in those cases – similar to those described in use cases 6 and 7 of the EDPB Recommendations 01/2020 – it could be difficult to identify effective supplementary measures given the particular circumstances of the processing.

### 3.2. Access by government authorities of a third country to data within the EU/scope of the GDPR

- Access requests issued by public authorities of third countries could also be addressed to CSPs established in the EU/EEA. In such cases, Article 48 GDPR should apply, providing for the safeguards necessary to ensure that the level of protection afforded by the GDPR would not be undermined. However, there could be an issue where the CSP receiving the request for access is part of a multinational group to which third country laws may apply. This may happen, in particular, taking into account the scope of certain foreign legislations, especially in the field of law enforcement or in the field of national security, which allow their public authorities to request access to data outside their own territory. Indeed, in these cases, requests can be addressed to companies which fall within the scope of these legislations. Therefore, in some situations, third countries' legislations deemed problematic in case of transfers would also apply within the EU/EEA and to data of EU/EEA data subjects without any initial transfer.

- GDPR provision involved: Articles 28 and 48.

- In this context, even where no data is transferred beforehand, the responsibility of PA could be engaged with regard to their CSPs on the basis of Article 28 which requires controllers to only use processors providing sufficient guarantees to implement appropriate technical and organisational

measures in such a manner that processing will meet the requirements of the Regulation and ensure the protection of the rights of the data subject.

- As a matter of fact, in their model contracts, almost all CSPs refer to the need to transfer personal data in order to 'comply with law'. However, in no case is it clarified which 'law' is referred to, i.e. if this refers to EU MS laws or the laws of other countries (and, in some cases, general information is provided to the PA in relation to the way in which those requests are processed and some safeguards put in place).

- Clauses of this kind carry a huge risk for the PA as they are often included in the model contracts as authorised exceptions to the requirement of processing personal data in the EEA region; therefore, they result in instructions to process personal data in a way that may undermine the level of protection afforded by the GDPR as far as they allow processors to abide by third country laws which may impose restrictions on data protection rights that are not proportionate and necessary in a democratic society. In this respect, it would be essential for the PA to identify exactly the possible cases at stake in order to ensure that the requirements of the Regulation (including a valid legal basis and the respect of Chapter V provisions for any transfer to be carried out, the transparency obligations, the security measures) will be met and the protection of the rights of the data subject ensured.

- Where those processing activities (i.e., the disclosure of personal data by the processor in case of request by a third country public authority) are not referred to in the contracts, it should be borne in mind that Article 28(3)a GDPR allows for processors not to operate on the controller's instructions only where required to do so by Union or Member State law (i.e., not by a third country law). Furthermore, Article 48 GDPR contains requirements that have to be met both by controllers and by processors and, as a matter of fact, are not referred to in the Data protection Agreements/addendums proposed by the CSPs.

- With regard to this issue, some mitigating factors identified by stakeholders for IaaS or PaaS services consist in adopting security measures such as encryption which may impede access to data in the clear if the decryption key is retained by the PA; however, such a mitigating factor cannot be adopted in case of SaaS services. Furthermore, there is a risk that no safeguards would be put in place if informing the controller on possible access requests by third country public authorities is prohibited beforehand (which could happen in most cases).

**4. <u>On telemetry data</u>**

**4.1. <u>Difficulties in identifying the personal data at stake and understanding the processing activities carried out by the CSP, including international transfers</u>**

- In order to provide the services, all CSPs collect and process telemetry data, i.e. data relating to the use of infrastructures and services (resource identifiers, tags, security and access roles, rules, usage policies, permissions, usage statistics) by different kind of users (e.g. employees, public Wi-Fi users, students, etc…). In particular, this data may be used e.g. to detect, identify and respond to operational issues, such as identifying and patching bugs and fixing problems, or to measure, support, and improve the services provided. Technical and organizational measures to protect personal data processed are generally adopted by the CSPs; data may be anonymized (e.g. by default avoiding the collection of personal data) or pseudonymized and rules are usually set forth in order to minimize human access to usage and diagnostic data and avoid the identification of individuals. However, from a data protection point of view, the exact role of the CSPs when processing this kind of data should be clarified. In some cases, they declare they act as controllers while in others they consider themselves as processors on behalf of the PA.

- GDPR provisions involved: Articles 5, 6, 28.

- In most cases, stakeholders do not appear to pay special attention to these processing activities and additional information was sought from the CSPs only because of the investigation activities. In some cases, the information provided was not precise enough and additional information was requested. However, considering the huge amount of personal data that may be collected, a more careful assessment on the part of the PA would be essential, in particular where telemetry data may be collected with regard to the end-user of the services (e.g. individuals to whom a service is provided by the PA). Clarifying the exact role played by the CSPs when processing telemetry data is essential in order to identify the appropriate legal basis and ensure the respect of Article 5 GDPR principles with particular regard to transparency, purpose limitation and data minimisation.

## 5. On Compliance

### 5.1. Audit

- As a preliminary result of the enforcement action, it seems to be a common approach for all involved stakeholders to carry out periodic checks on CSPs' activities through the annual verification of the certification reports and the documentation made available by the CSP on the website; by analysing the security reports of independent bodies; or via checklists prepared by the PA to assess the compliance by the CSP with the contractual clauses and current legislation on the processing of personal data. Thus, it appears that, so far, no public authority has carried out specific and direct audit activities, including inspections, regarding any CSPs.

- GDPR provision involved: Article 5(2) and 28(3)(h).

- Some stakeholders complained that generally the CSPs do not allow the performance of audits by customers and that it is difficult to negotiate specific clauses in this regard (such as obtaining access to the results of audits carried out by third parties or requesting that third parties focus their audit on specific aspects indicated by the PA).

### 5.2. Record of processing activities of the CSP in relation to the specific controller/public administration

- As a preliminary result of the enforcement action, it appears that CSPs do not hold a specific record of processing activities carried out on behalf of each PA. When a record of the processing activities is in place, it is of a general nature and refers to all the activities carried out by the processor in relation to the services provided to all customers/controllers.

- GDPR provision involved: Article 30(2).

- Upon specific requests, some CSPs did not reply, others referred to their own websites for information on the processing activities carried out, others sent a very general record which did not contain all of the elements set forth by Article 30(2) (a-d) GDPR,

- In one case, it was also considered that it was not possible for the CSP to hold a record of the specific processing activities for each customer, since the CSP had no information on the types/categories of the processed data, nor of the purposes of the processing and the services actually used by customers (it was explicitly considered that the CSPs do not restrict the publicly available services the customer may choose to use).

## Part III – Actions by the SA

1. **Have you taken action (i.e. fact-finding exercises, informal contact, prior consultation, investigation) towards any of the stakeholders concerning the use of cloud-based services *prior to* launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

- Prior to launching the coordinated action, the IT SA has adopted the following decisions in the field of cloud computing:

- On 23 November 2021[41], the IT SA issued a favorable opinion, with some comments, on a draft Decree of the Ministry of Foreign Affairs on the testing of electronic voting in elections for the renewal of Committees of Italians Abroad. In issuing the opinion, the Authority requested clarifications in the decree about the role carried out by the Ministry and other parties involved (e.g. Cloud service provider) and highlighted the need to envisage the data retention period of data. Besides, the Ministry was also required to take additional measures in case of transfer of personal data in third countries to ensure a level of protection of personal data substantially equivalent to that provided for in the EU, including the encryption of personal data by the controller, with encryption keys in its exclusive availability.

- On 16 September 2021[42], in a decision on a complaint relating to the 'proctoring system' called Respondus used by an Italian University, the IT SA declared the unlawfulness of the processing carried out by the University on account of the infringement of Articles 5 (1) (a), (c) and (e), 6, 9, 13, 25, 35, 44 and 46 of the GDPR and Section 2-f of the Italian Data Protection Code and prohibited the University from further processing students' biometric data and data on the basis of which the profiling of data subjects through the Respondus system is carried out. The Authority prohibited also the transfer of data subjects' personal data to the United States of America in the absence of adequate safeguards for such data subjects as a result of the absence of an appropriate and documented assessment of the relevant third country law in the light of the Schrems II ruling and issued a fine of EUR 200.000,00 (two hundred thousand).

- In June 2021[43], as a result of an on own volition enquiry, the IT SA found infringements of the GDPR arising from the configuration of the 'IO' app, a public administration app used as access point to local and national public services in Italy (among others, for example, related to payments towards PAs, EU Digital COVID certificates, communication from PAs to citizen, etc.), in relation to excessive data collection and transfer to third countries, inadequate information to users, failure to request users' consent for storing information, or accessing information that is already stored, in their terminal equipment, unnecessary geolocation of users based on IP addresses. The Garante ordered to provisionally limit certain data processing activities as performed via the said app since they entailed interactions with services by Google and Mixpanel and resulted accordingly into transfers to third countries of data that are highly sensitive including information on cashback transactions and payment tools. After the publicly-owned company managing the App committed themselves to minimize user data collected for the purpose of activating the

[41] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9721434

[42] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9703988. The decision is currently under judicial proceeding.

[43] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9668051 and https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9670061(

services provided through the 'IO' app and transferred to third countries and to implement the corrective measures requested by the SA (e.g. several functions were deactivated as they allowed tracing user location via his or her IP address and unnecessary Google services were deactivated and steps were taken to prevent the contents of push notifications from being disclosed to Google and Apple), the Italian SA lifted the temporary limitation it had imposed on the processing of personal data. However, the processing will continue to be limited as for the data collected and stored by Mixpanel. Those data may not be used any longer and will only be stored by the company until the SA completes its investigations (which are still ongoing).

- In January 2020[44], the IT SA issued an opinion on the draft "Guidelines — Security in ICT procurement" setting out general guidelines for public administrations when dealing with IT acquisitions as well as public service providers. Among several recommendations, the Garante highlighted the need to adequately identify, as part of the tender specifications, a correct distribution of the respective responsibilities between the controller and processors, in particular avoiding disproportionate clauses relating to liability, especially in the case of standard contracts, with almost zero trading margins on the part of the data controller.

2. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (E.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**

- The investigations are still pending.

## Part IV – Other

1. **What is your general impression of the levels of awareness and compliance of the stakeholders you consulted concerning the use of cloud?**

- It seems that there is generally a lack of awareness about: 1. data transfers that can take place even despite the PA has identified the EEA as the selected region for the main processing activities; 2. the telemetry data processed by the CSPs; 3. Request for access to personal data stored in the EEA by third country public authorities.

2. **Are there any other issues or topics that you would like to flag?**

- None.

3. **Are there any leading practices of the stakeholders you have contacted that you would like to share?**

- None for the time being.

[44] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9283857

# LI SA

## Datenschutzstelle Fürstentum Liechtenstein

### Part I – Statistics

**4. <u>How many stakeholders have you contacted within the following categories?</u>**

- Ministry of the central government
- Independent public body of the central government
- Buyer for the central government (1)
- Publicly-owned company acting as a processor for several central public bodies
- Ministry of the regional government
- Independent public body of the regional government
- Buyer for the regional government
- Publicly-owned company acting as a processor for several regional public bodies
- Other, please specify

**5. <u>How many stakeholders have you contacted within the following sectors?</u>**

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government
- Economic affairs
- Education
- Finance
- Health
- Infrastructure
- Employment
- Justice
- Tax
- Other, please specify: **We did not contact a stakeholder from a specific sector, but the IT department as the buyer for the central government.**

**6. <u>If you have contacted a buyer, for which sectors does this buyer provides its services:</u>**

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government
- Economic affairs
- Education
- Finance
- Health
- Infrastructure
- Employment
- Justice
- Tax
- **No specific sector**
- Other, please specify

**7. <u>If you have contacted a buyer, and if you have this information, please specify the number of stakeholders this buyer provides services for:</u>**

- 39 departments

8. **What was the initial procedural framework of your action?**

- **Fact finding**
- Fact finding + determining follow-up action based on the results
- New investigation[45]
- Ongoing investigation

9. **How many stakeholders indicated that they use CSPs or are planning to do so in the near future (end of 2022)?**

- The central buyer gave us 5 examples of CSPs that are used or planned to be used in the near future.

10. **Of the stakeholders that use CSPs (or are planning to do so in the near future), how many use CSPs for the following functions?**

- Internal organisation (office suites, internal communication, HR, etc.): **All 5 CSPs examined**
- Exercise of public functions (services to citizens, processing citizen's data, etc.)

11. **For the following commonly identified sectors, please specify if any hyper-scalers[46] are involved (if so please name them) either because they provide the services themselves or because the services are using the infrastructures of these hyper-scalers**

- Health
- Finance
- Tax
- Education
- Central buyers or providers of IT services: **Cloud services of Microsoft and AWS are (planned to be) used.**

12. **How many stakeholders took the following actions prior to- or during the acquisition of a CSP?**

- Perform a DPIA: **Only for one CSP, a DPIA was performed.**
- Does the DPIA analyse transfers in details (sometimes called DTIA): **No, however, for a second CSP a risk-based analysis of transfers was performed (Rosenthal).**
- Contact the DPO for advice: **Yes.**
- Perform a general risk analysis: **A general risk analysis is being performed for every CSP procured.**
- Contact the SA for advice: **The SA was contacted regarding 1 CSP that is planned to be used.**

13. **How many stakeholders (including buyers) take the following actions during the use of the CSP?**

- Monitoring technical and organisational measures to ensure compliance: **When procuring the CSP, monitoring of technical and organisational measures to ensure compliance is performed. After that, monitoring is only performed in a non-systematic way (ad hoc), e.g. when a technical issue comes up, a legal decision becomes known, a new version of an application is rolled out, new categories of data are processed, etc.**
- In case of transfers, adopting technical and organisational measures, including supplementary measures, where needed, and monitoring if changes in the regulatory landscape occur (e.g. Schrems II): **When procuring the CSP, technical and organisational measures such as encryption (data in transit, data at rest and key management), server location, identity access**

[45] making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred

[46] Hyper-scalers provide cloud services at scale. It refers usually to the big cloud providers (Google, AWS, Microsoft …) on which other services may also depend

**management, Cloud Access Security Broker (CASB) services are planned or have already been implemented. After that, adoption of technical and organisational measures and monitoring are only performed in a non-systematic way (see above).**

- Regular risk assessments: **When procuring the CSP, a risk assessment is performed. After that, risk assessment is only performed in a non-systematic way, not on a regular base (see above).**

## Part II – Substantive issues

### 1. Pre-contractual phase: Determining sufficient guarantees with regards to appropriate technical and organisational measures

#### 1.1. Brief description:

- The central buyer tries to implement appropriate technical and organisational measures to ensure compliance of the CSP selected with GDPR. In particular, the central buyer tries to make sure that the location of the server is in Europe and that adequate encryption technologies are applied (data in transit/ data at rest). In addition, identity access management (IAM) and Cloud Access Security Broker (CASB) services are planned or have already been implemented. Whether these measures can be seen as sufficient in the context of international data transfers has to be further investigated. In addition, some contracts seem to allow the CSPs (and/or their sub-processors) to process large amounts of personal data other than the user data, e.g. telemetry data, for their own purposes and at locations elsewhere than where the server of the user data is located. It still has to be clarified, whether there are sufficient guarantees with regards to appropriate technical and organisational measures in all of the contracts and/or in the buying-process, ensuring protection of all personal data processed.

#### 1.2. Provision(s) of the GDPR (or national laws) concerned:

- A processing of personal data for own purposes of the CSP without a legal base would infringe Art. 5 (1) a and Art. 6 (1) GDPR.
- A transfer of such data to third countries without any/sufficient guarantees according to chapter V GDPR would infringe Art. 44 GDPR.
- A lack of appropriate technical and organisational measures would infringe Art. 24 (1) and (2), Art. 25 as well as Art. 32 GDPR.
- A lack of sufficient guarantees thereof in the contract would infringe Art. 28 GDPR.

#### 1.3. Why this has been an issue:

- It has to be clarified, how the central buyer can be supported in the pre-contractual phase, to avoid potential issues when determining sufficient guarantees with regards to appropriate technical and organisational measures.

#### 1.4. (Potential) solution(s):

- Central buyer: If it were established, that in any of the contracts with CSPs there are not sufficient guarantees with regards to appropriate technical and organisational measures, these contracts would have to be renegotiated to ensure compliance with GDPR of all data processing involved. In cases where this were not possible, the use of the CSP (or projects to use a certain CSP) would have to be terminated.
- Central buyer: Additional support in analysing and understanding contracts offered by CSPs and legal frameworks involved could be provided by a legal officer specifically in charge of this task. The legal officer could then also help negotiating GDPR-compliant contracts and implementing sufficient guarantees with regards to appropriate technical and organisational measures.

- Central buyer: The DPO should play an active role in the analysis and negotiation of contracts offered by CSPs as well.
- SA: The SA will continue to raise awareness regarding the issues and risks associated with the use of CSPs and stands ready to give advice to the central buyer.

**2. Contract with CSP: Risk mitigating measures within the contract**

**2.1. Brief description:**

- The central buyer tries to implement risk-mitigating measures within the contracts with CSPs. In particular, the central buyer tries to make sure that the location of the server is in Europe and that adequate encryption technologies are applied (data in transfer/ data at rest). However, especially with regards to US-based CSPs, the central buyer repeatedly finds itself in the situation that it either has to accept the terms offered in the contract by the CSP or has to withdraw, as there is no possibility to negotiate additional risk mitigating measures with the CSP. Furthermore, some of the contracts with the CSPs seem to allow the CSPs (and/or their sub-processors) to process large amounts of personal data other than the user data, e.g. telemetry data, for their own purposes and at locations elsewhere than where the server of the user data is located. It has to be clarified yet, whether there are enough risk mitigating measures incorporated within all of the contracts, ensuring adequate protection of data.

**2.2. Provision(s) of the GDPR (or national laws) concerned:**

- A processing of personal data for own purposes of the CSP without a legal base would infringe Art. 5 (1) a and Art. 6 (1) GDPR.
- A transfer of such data to third countries without any/sufficient guarantees according to chapter V GDPR would infringe Art. 44 GDPR.
- A lack of (sufficient) risk mitigating measures would infringe Art. 24 (1) and (2), Art. 25 as well as Art. 32 GDPR.
- A lack of them within the contract with a CSP would also infringe Art. 28 GDPR.

**2.3. Why this has been an issue:**

- The central buyer of the Principality of Liechtenstein is a rather small customer of CSP services. Because of this, it does not have sufficient negotiating power when it comes to terms and conditions offered in contracts of big CSPs. Therefore, the central buyer repeatedly finds itself in the situation that it can either accept contracts that do not contain sufficient risk mitigating factors or has to withdraw. It has to be clarified, how the central buyer can be supported in negotiating adequate risk mitigating measures with a CSP.

**2.4. (Potential) solution(s):**

- Central buyer: If it were established, that any of the contracts with CSPs do not contain sufficient risk mitigating measures, these contracts with CSPs would have to be renegotiated to ensure compliance with GDPR of all data processing involved. In cases where this was not possible, the use of the CSP (or projects to use a certain CSP) would have to be terminated.
- Central buyer: Additional support in analysing and understanding contracts offered by CSPs and legal frameworks involved could be provided by a legal officer specifically in charge of this task. The legal officer could then also help negotiating adequate risk mitigating measures within the contract with a CSP.
- Central buyer: The DPO should play an active role in the analysis and negotiation of contracts offered by CSPs as well.
- SA: The SA will continue to raise awareness regarding the issues and risks associated with the use of CSPs and stands ready to give advice to the central buyer.

## 3. Contract with CSP: Negotiating a bespoke contract

### 3.1. Brief description:

- The central buyer tries to negotiate bespoke contracts with CSPs. It has done so successfully, e.g. when negotiating that the location of the server is in Europe and that adequate encryption technologies are applied (data in transfer/ data at rest). On other occasions, however, especially with US-based CSPs, the central buyer apparently found itself in the situation that it could either accept the terms and conditions offered in the contract by the CSP or had to withdraw, as there was no possibility to negotiate additions or amendments to it. As a result, some contracts were not closed at all and others are not fully tailor-made to the needs of the central buyer, but reflect (in parts) the non-negotiable clauses offered by the CSP (and/or its sub-processors). It has to be further investigated yet, whether these pre-specified clauses ensure adequate protection of data.

### 3.2. Provision(s) of the GDPR (or national laws) concerned:

- A processing of personal data for own purposes of the CSP without a legal base would infringe Art. 5 (1) a and Art. 6 (1) GDPR.
- A transfer of such data to third countries without any/sufficient guarantees according to chapter V GDPR would infringe Art. 44 GDPR.
- A contract with a CSP not covering all the data protection requirements according to GDPR would infringe Art. 28 GDPR.

### 3.3. Why this has been an issue:

- The central buyer of the Principality of Liechtenstein is a rather small customer of CSP services. Because of this, it does not have sufficient negotiating power when it comes to terms and conditions offered in contracts of big CSPs. Therefore, it repeatedly found itself in the situation that it could either accept (parts of) pre-specified contracts or had to withdraw. It has to be clarified, how the central buyer can be supported in negotiating bespoke contracts with CSPs.

### 3.4. (Potential) solution(s):

- Central buyer: If it were established, that any of the contracts / clauses in contracts with CSPs do not fully respond to the requirements of the central buyer, these contracts / clauses in contracts with CSPs would have to be renegotiated to ensure GDPR-compliance for all data processing involved. In cases where this were not possible, the use of the CSP (or projects to use a certain CSP) would have to be terminated.
- Central buyer: Additional support in analysing and understanding contracts offered by CSPs and legal frameworks involved could be provided by a legal officer specifically in charge of this task. The legal officer could then help negotiating bespoke clauses within the contract with a CSP.
- Central buyer: The DPO should play an active role in the analysis and negotiation of contracts offered by CSPs as well.
- SA: The SA will continue to raise awareness regarding the issues and risks associated with the use of CSPs and stands ready to give advice to the central buyer.

## 4. International transfers and access by foreign public authorities: transfer awareness

### 4.1. Brief description:

- The central buyer tries to handle international data transfers and the potential access by foreign public authorities according to the requirements of GDPR. He does that primarily by choosing European CSPs or in establishing that at least the location of the server is in Europe and that adequate encryption technologies are applied (data in transfer/ data at rest). Beyond that, the central buyer tends to apply a risk-based approach to evaluate the sensitivity of the data processed by the CSP and the legal framework of the country of the CSP. Besides, the answers to the questionnaire seem to indicate that the central buyer might not be fully aware that some

European CSPs use sub-processors (especially US-based CSPs) that are processing personal data for own purposes as well and/or transfer them to third countries. Furthermore, some contracts with the CSPs also allow the CSPs (and/or their sub-processors) to process large amounts of personal data other than the user data, e.g. telemetry data, for their own purposes and at locations elsewhere than the server of the user data. As a result, it has to be investigated whether there are sufficient safeguards according to chapter V GDPR in all of the contracts for the adequate protection of data. It seems to be the case therefore, that transfers of personal data to third countries are taking place in some of the contracts and potential access by foreign public authorities to the data cannot be excluded. This is subject to further investigation, however.

**4.2. Provision(s) of the GDPR (or national laws) concerned:**

- A transfer of personal data to third countries without any/sufficient guarantees according to chapter V GDPR would infringe Art. 44 ff. GDPR.
- A transfer /disclosure of personal data to foreign public authorities might also infringe Art. 48 GDPR.
- A potential access to personal data by foreign public authorities might – under certain circumstances – infringe Art. 5 (1) f GDPR.
- A selection of a processor/sub-processor who cannot adhere to the principles of GDPR would infringe Art. 28 (1) and (3) a GDPR.

**4.3. Why this has been an issue:**

- Every time the central buyer did not find an equivalent European CSP to a third country-CSP, it tried to mitigate the risks of the data processing / transfers and of potential access by foreign public authorities as far as possible (e.g. server location in Europe, encryption of data, IAM and CASB solutions, processing of non-sensitive data only, etc.). However, according to the answers to the questionnaire, the central buyer seems to only have assessed the actual CSP and its data processing, but not all the sub-processors used by a CSP as well. Neither does the central buyer seem to have assessed the potentially abundant data processing for own purposes of some CSPs (and/or their sub-processors) and in third countries (e.g. telemetry data), which also could involve international data transfers.
- In order to establish, whether these presumed shortcomings come true and whether the risk mitigating measures taken by the central buyer are sufficient to ensure adequate protection of the (transferred) personal data, a further in-depth investigation will be required. Furthermore, it has to be clarified, how the central buyer can be supported in raising its awareness of international data transfers and of (potential) access by foreign public authorities as well as of the risks/issues associated with it.

**4.4. (Potential) solution(s):**

- Central buyer: If it were established, that any of the contracts with CSPs comprise international data transfers that do not comply with chapter V GDPR, these contracts with CSPs would have to be renegotiated to ensure compliance with GDPR of all data processing involved. In cases where this were not possible, the use of the CSP (or projects to use a certain CSP) would have to be terminated.
- Central buyer: Additional support in analysing and understanding contracts offered by CSPs and legal frameworks involved could be provided by a legal officer specifically in charge of this task. The legal officer could then also help negotiating GDPR-compliant contracts covering all data processing foreseen in them.
- Central buyer: The DPO should play an active role in the analysis and negotiation of contracts offered by CSPs as well.

- SA: The SA will continue to raise awareness regarding the issues and risks associated with the use of CSPs and stands ready to give advice to the central buyer.

**5. Telemetry data**

**5.1. Brief description:**

- The central buyer sincerely tries to negotiate GDPR-compliant contracts with CSPs. He does that primarily by establishing that the location of the server is in Europe and that adequate encryption technologies are applied (data in transfer/ data at rest). In addition, identity access management (IAM) and Cloud Access Security Broker (CASB) services are planned or have already been implemented. However, some contracts with the CSPs seem to allow that the CSPs (and/or their sub-processors) process large amounts of personal data other than the user data, e.g. telemetry data, for their own purposes and at locations elsewhere than the server of the user data. As a result, it has to be further investigated whether there are enough guarantees found in some of the contracts, ensuring adequate protection of those data as well.

**5.2. Provision(s) of the GDPR (or national laws) concerned:**

- A processing of personal data, such as telemetry data, for own purposes of the CSP without a legal base would infringe Art. 5 (1) a, b, c and Art. 6 (1) GDPR.
- A transfer of such data to third countries without any/sufficient guarantees according to chapter V GDPR would infringe Art. 44 GDPR.
- A lack of adequate data protection clauses covering also telemetry data in the contract with a CSP would infringe Art. 28 GDPR.

**5.3. Why this has been an issue:**

- It has to be clarified, how the central buyer can be supported to avoid potential issues regarding the processing of telemetry data by CSPs (and/or their sub-processors).

**5.4. (Potential) solution(s):**

- Central buyer: If it were established, that any of the contracts with CSPs comprise an unlawful processing of telemetry data by the CSP (and/or its sub-processors), these contracts with CSPs would have to be renegotiated to ensure GDPR-compliance for all data processing involved, including processing of telemetry data. In cases where this were not possible, the use of the CSP (or projects to use a certain CSP) would have to be terminated.
- Central buyer: Additional support in analysing and understanding contracts offered by CSPs and legal frameworks involved could be provided by a legal officer specifically in charge of this task. The legal officer could then also help negotiating GDPR-compliant clauses concerning the processing of telemetry data by the CSP.
- Central buyer: The DPO should play an active role in the analysis and negotiation of contracts offered by CSPs as well.
- SA: The SA will continue to raise awareness regarding the issues and risks associated with the use of CSPs and stands ready to give advice to the central buyer.

## Part III – Actions by the SA

**1. Have you taken action (i.e. fact-finding exercises, informal contact, prior consultation, investigation) towards any of the stakeholders concerning the use of cloud-based services *prior to* launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the stakeholder, general guidance,**

**corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

- We have roughly outlined the data protection related risks and issues connected to the use of MS 365 in the framework of a general risk analysis performed by the central buyer.

2. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (E.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing).**

- We plan to inform the central buyer of the results of the CEF and thus of the general direction of dealing with CSPs in the EEA as defined by the EDPB. This should raise awareness, but also provide legal guidance and negotiating power for the central buyer when assessing / procuring CSPs.

## Part IV – Other

1. **What is your general impression of the levels of awareness and compliance of the stakeholders you consulted concerning the use of cloud?**

- Compliance is very good in several areas, but in other areas there seem to be some gaps and further investigation has to be performed. Besides, as there is no established European best practice regarding CSPs like MS 365 etc. yet, the central buyer tends to apply mainly a risk-based approach with regards to international data transfers.

2. **Are there any other issues or topics that you would like to flag?**

- No

3. Are there any leading practices of the stakeholders you have contacted that you would like to share?

- No

# LT SA

## State Data Protection Inspectorate (hereinafter – Lithuanian SA)

### Part I – Statistics

1. **How many stakeholders have you contacted within the following categories?**

- 1. Independent public body of the central government

2. **How many stakeholders have you contacted within the following sectors?**

- Other, please specify: 1. Statistics Lithuania (hereinafter – stakeholder)

3. **If you have contacted a buyer, for which sectors does this buyer provides its services:**

- N/A

4. If you have contacted a buyer, and if you have this information, please specify the number of **stakeholders this buyer provides services for:**

- N/A

5. **What was the initial procedural framework of your action?**

- Fact finding + determining follow-up action based on the results
- Ongoing investigation

6. **How many stakeholders indicated that they use CSPs or are planning to do so in the near future (end of 2022)?**

- 1

7. **Of the stakeholders that use CSPs (or are planning to do so in the near future), how many use CSPs for the following functions?**

- Internal organisation (office suites, internal communication, HR, etc.) : **1**
- Exercise of public functions (services to citizens, processing citizen's data, etc.): **1**

8. **For the following commonly identified sectors, please specify if any hyper-scalers[47] are involved (if so please name them) either because they provide the services themselves or because the services are using the infrastructures of these hyper-scalers:**

- Health
- Finance
- Tax
- Education
- Central buyers or providers of IT services

- CSP Palantir uses Amazon Web Services, Inc. (AWS) and Microsoft Corporation. AWS provides the cloud infrastructure for Palantir products. Microsoft Corporation uses for provision of cloud infrastructure to host Active Directory for CentralAuth.
- CSP Microsoft provides the services themselves.

9. **How many stakeholders took the following actions prior to- or during the acquisition of a CSP?**

[47] Hyper-scalers provide cloud services at scale. It refers usually to the big cloud providers (Google, AWS, Microsoft …) on which other services may also depend

- Perform a DPIA: **none**
- Does the DPIA analyse transfers in details (sometimes called DTIA): **none**
- Contact the DPO for advice: **none**
- Perform a general risk analysis: **none**
- Contact the SA for advice: **none**

**10. How many stakeholders (including buyers) take the following actions during the use of the CSP?**

- Monitoring technical and organisational measures to ensure compliance: **none**
- In case of transfers, adopting technical and organisational measures, including supplementary measures, where needed, and monitoring if changes in the regulatory landscape occur (e.g. Schrems II): **none**
- Regular risk assessments: **none**

## Part II – Substantive issues

**1. Data protection impact assessment (Article 35 GDPR).**

**1.1. Name the issue and briefly describe the main issue(s) identified.**

- The audited stakeholder uses the services of three CSPs for data processing:
  - The stakeholder has concluded Palantir Foundry (a cloud-based database management platform) licensing agreement with CSP Palantir Technologies UK, Ltd., including platform support, along with infrastructure services.
  - Services provided by Microsoft Corporation include Office program data synchronization / transfer services – e-mail and group work data exchange service, website and workspace hosting service, communication service, user data cache (products as Office 365, OneDrive, Teams).
  - Services provided by CSP Information Society Development Committee (CSP ISDC) (public institution under the Ministry of Economy and Innovation of the Republic of Lithuania) are used for internal administration and public functions (contracts, information systems administration, statistical surveys, human resources management).
- In none of the three cases data protection impact assessment (DPIA) has been carried out.

**1.2. Which provision(s) of the GDPR (or national laws) does this concern?**

- According to GDPR Article 35 (3) (b) a DPIA referred to in paragraph 1 shall in particular be required in the case of processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10. In the information systems, the data of which is processed on the cloud-based platforms, personal data is processed on a large scale, and cloud services are used for processing personal data, which can be evaluated as an innovative technology for data processing. It should be noted that the information systems process on a large-scale personal data of extremely vulnerable data subjects and special personal data categories such as special categories of data referred to in GDPR Article 9(1) (for example, health data) and personal data relating to criminal convictions and offences referred to in GDPR Article 10. The exceptions specified in Articles GDPR Article 35 do not apply, therefore Lithuanian Department of Statistics had the obligation to perform DPIA in all three cases before starting to use services based on cloud technology for processing personal data.

**1.3. Explain why this has been an issue for your stakeholders?**

- Stakeholder takes the position that the technical and organizational measures applied by CSPs are sufficient and an assessment of the impact on data protection was not required, and this stakeholder also expressed the opinion that DPIA is not required when standard contractual conditions are applied.

**1.4. What are differences that you have encountered between stakeholders in your Member State?**

- N/A. Lithuanian SA inspected only one stakeholder.

**1.5. What are solutions to this issue? Please describe if these solutions are already implemented or potential, and whether this solution is provided by the SA or the stakeholders.**

- Lithuanian SA proposes to establish an obligation to carry out DPIA (GDPR Article 35(1)) and, if necessary, its review (GDPR Article 35(11)).

**2. Problems with choosing specific CSPs and no contract negotiations.**

**2.1. Name the issue and briefly describe the main issue(s) identified.**

- **Issue (1)** - CSP Palantir and CSP Microsoft terms of the contracts for cloud services were negotiated, they were accepted on a take-it-or-leave-it basis:
    - Pursuant to Palantir's declaration of exclusivity, in which Palantir together with all of its group companies and affiliates, affirms that it is the sole supplier of Palantir software (including Palantir Foundry) to the government and has an exclusive license to sell, install, support and update such software, Lithuanian SA found that the stakeholder did not select or evaluate any other cloud service providers. I.e., The State Data Management information system has been created on the basis of the Data management and analytics platform – Palantir Foundry, so the stakeholder has no other CSP option for this information system.

    - A Microsoft licensing agreement has been concluded with private company (not Microsoft). Since Microsoft license can only be purchased based on a standard contract, negotiations were not carried out. 2010 SCCs of Microsoft Corporation apply, Stakeholder has no direct written data processing agreement with Microsoft.

    - This indicates that the Stakeholder could not negotiate with the CSP on the terms of the contract in order to properly adjust the terms of the contract that they meet Stakeholder's requirements, and in the contracts, there are indicated possibilities to object on subproviders, but there are no provisions on the consequences of this objection (GDPR Article 28(2)). It is not clear whether the objection can be expressed without breaching the contract.

- **Issue (2)** – Sub-processors. Stakeholder has informed Lithuanian SA that it does not have any information/evidence that CSPs Palantir and CSP ISDC are actually using services of sub-processors based on contracts or other legal act in compliance with the provisions of the GDPR Article 28(4).

**2.2. Explain why this has been an issue for your stakeholders?**

- **Issue (1)** – On the date of stakeholder signing Microsoft licencing agreement where 2010 SCCs apply, 2021 SCCs have already been approved by the EC, therefore stakeholder cannot be sure that data processing by Microsoft is sufficiently safe.

Stakeholder holds the position that they were in a position where they had to accept contracts on a take-it-or-leave-it basis without having power to negotiate.

- **Issue (2)** - Stakeholder may not have requested detailed and clear information /did not contact directly the CSPs Palantir and CSP ISDC about the verification of compliance with the GDPR Article 28(4).

**2.3. Which provision(s) of the GDPR (or national laws) does this concern?**

- **Issue (1)** - GDPR Article 28(2): The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

  GDPR Article 28(3) states that Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.

  GDPR Article 28(9): The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.

- **Issue (2)** -According to GDPR Article 28(4), CSP must provide sufficient guarantees that sub-processors implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation and Stakeholder.

**2.4. What are solutions to this issue? Please describe if these solutions are already implemented or potential, and whether this solution is provided by the SA or the stakeholders.**

- **Issue (1)** - Stakeholder should evaluate if CSP SCCs meet the requirements of GDPR and Stakeholder's requirements. Stakeholder must ensure compliance with the provisions of GDPR Article 28.

- **Issue (2)** – Stakeholder should be guaranteed that CSP's sub-processors implements appropriate technical and organisational measures in such a manner that the processing will meet the requirements of GDPR and Stakeholder's requirements.

**3. International transfers and access by foreign public authorities.**

**3.1. Name the issue and briefly describe the main issue(s) identified.**

- Lithuanian SA was provided with only minimal information on the transfer of personal data to third countries and only on transfers to the US in the case of using CSP Palantir services. Stakeholder could not explain what personal data is transferred to the third countries, what technical and organizational measures are applied for such transfers.

- Stakeholder did not provide any information whether in the case of CSP Microsoft and CSP ISDC provided cloud services personal data is transferred to third countries.

**3.2. Explain why this has been an issue for your stakeholders?**

- Stakeholder indicated that standard data protection conditions are used for the transfer of personal data to third countries, but the EU SCCs that provide specific guarantees around transfers of personal data for in-scope services were not signed with CSP Palantir. Therefore, Lithuanian SA considers that failure to sign SCCs (2021) with Palantir does not obligate unconditional compliance with them and decent level of security.

- Stakeholder may not have requested detailed and clear information /did not contact directly the CSPs Microsoft and CSP ISDC on a matter of personal data transfers to the third countries.

**3.3. Which provision(s) of the GDPR (or national laws) does this concern?**

- GDPR Article 46(1): In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

**3.4. What are solutions to this issue? Please describe if these solutions are already implemented or potential, and whether this solution is provided by the SA or the stakeholders.**

- Lithuanian SA proposes to sign EU SCCs (2021) for the transfers of personal data to the third countries with the CSP Palantir in order to provide specific guarantees around transfers of personal data for cloud-based services.

- Verifying whether personal data is actually transferred to third parties using cloud services of CSP Microsoft and CSP ISDC. In the case of transfers implement the adequate measures in order to ensure compliance with the provisions of GDPR Chapter V.

**4. Collection and processing by the CSP of diagnostic/telemetry data (Article 5 GDPR).**

**4.1. Name the issue and briefly describe the main issue(s) identified.**

- *CSP* Palantir collects and processes diagnostic / telemetric data (metrics, analysis, statistics, or other data) related to the stakeholder's use of the software (in case this data is anonymized).

- *CSP* Microsoft collects and manages diagnostic / telemetric data (providing users with unique IDs).

- Stakeholder did not provide / specify the categories of personal data collected regarding the telemetric/diagnostic data processed by the *CSP* Palantir to Lithuanian SA.

- Stakeholder did not conduct an assessment of the data (including diagnostic / telemetric data) used by *CSP* Palantir and *CSP* Microsoft for their own purposes, nor did it specify where the anonymization is performed (on the client or on the *CSP* servers).

**4.2. Which provision(s) of the GDPR (or national laws) does this concern?**

- The principles of Article 5 of the GDPR that personal data must be processed in a lawful, fair and transparent manner in relation to the data subject (principle of lawfulness, fairness and transparency), collected for specified, clearly defined and legitimate purposes and not further processed in a manner incompatible with those purposes are not guaranteed, implemented. adequate, appropriate and limited to what is necessary to achieve the purposes for which they are processed (principle of data minimisation).

**4.3. Explain why this has been an issue for your stakeholders?**

- Because stakeholder may not have requested detailed and clear information /did not contact directly the CSP about the diagnostic / telemetric data being collected and processed. They were not analysed, nor were there any evaluations carried out before the start of usage, and in the contract did not provide clearly and precisely what could be collected.

**4.4. <u>What are differences that you have encountered between stakeholders in your Member State?</u>**

- N/A.

**4.5. <u>What are solutions to this issue? Please describe if these solutions are already implemented or potential, and whether this solution is provided by the SA or the stakeholders.</u>**

- A possible solution is to clearly provide in the CSP Palantir contract what diagnostic / telemetric data can be processed and when. Conduct a thorough assessment of them, requiring evidence from the CSP Palantir and CSP Microsoft. This decision is provided for by the Inspectorate, but has not yet been submitted to the stakeholder, and therefore has not been implemented.

**5. <u>Monitoring of the implemented technical and organisational measures including security measures of the CSPs (Article 32 GDPR).</u>**

**5.1. <u>Name the issue and briefly describe the main issue(s) identified.</u>**

- Stakeholder has not provided / submitted to Lithuanian SA any data safety risk assessment related to the stakeholder, which led to the fact that CSP Palantir, CSP Microsoft is the right solution for the stakeholder.

- Stakeholder did not provide any evidence to evaluate the CSP Palantir and CSP Microsoft, and the stakeholder did not provide any information to familiarize itself with the certification reports or summaries of the report of the CSP Palantir and CSP Microsoft.

- The stakeholder did not provide information / evidence that the CSP Palantir provides adequate organizational and technical security measures. The stakeholder did not provide a document or other evidence of what exactly technical and organizational measures are implemented. The stakeholder did not provide information / evidence regarding the technical and organizational security measures implemented by CSP Palantir, or after conducting a risk assessment.

- Stakeholder has indicated that there is currently no monitoring of the application of technical and organizational measures with regard to the CSP Microsoft.

- The stakeholder does not carry out / does not conduct ongoing data protection risk assessments, including information security risk assessments (ex-post) related to the implementation of cloud computing (CSP Palantir and CSP Microsoft).

**5.2. <u>Which provision(s) of the GDPR (or national laws) does this concern?</u>**

- The principles of Article 24 and Article 32 of the GDPR are not guaranteed, implemented, that, taking into account the nature, scope, context and purposes of the processing, as well as the risks of varying probability and seriousness to the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and be able to demonstrate that the data are processed in accordance with this Regulation. Those measures shall be reviewed and updated as necessary. And the establishment of an adequate level of security shall take into account, in particular, the risks arising from the processing, in

particular the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or unauthorised access to data transmitted, stored or otherwise processed.

**5.3. Explain why this has been an issue for your stakeholders?**

- This caused problems because the stakeholder did not provide the assessments carried out by the CSP, DPIA, did not carry out a risk assessment, did not provide an assessment of the technical and organizational security measures implemented by the CSP, or other evidence based on which it could be said that the CSP ensure an adequate level.

**5.4. What are differences that you have encountered between stakeholders in your Member State?**

- N/A.

**5.5. What are solutions to this issue? Please describe if these solutions are already implemented or potential, and whether this solution is provided by the SA or the stakeholders.**

- A possible solution is to clearly identify, listing the technical and organisational security measures to be implemented by CSP and to carry out a thorough assessment of them, requiring CSP to demonstrate compliance. This decision is provided for by the Lithuanian SA, but has not yet been submitted to the stakeholder, and therefore has not been implemented.

**6. Process to deal with data breaches and notifications (Articles 33 and 34 GDPR).**

**6.1. Name the issue and briefly describe the main issue(s) identified.**

- The agreement between CSP Palantir and the stakeholder did not address the provisions for reporting a personal data breach and cyber incidents and the timing of the response to them.

- The stakeholder has submitted to Lithuanian SA an addendum containing the 2010 SSC CSP Microsoft, which provides for the immediate notification of a personal data breach to the stakeholder, but the exact time is not provided, and also provides that the notice must contain mandatory information under Article 33 of the GDPR, but does not specify exactly what information is to be provided.

**6.2. Which provision(s) of the GDPR (or national laws) does this concern?**

- The principles of Articles 33 and 34 GDPR that, in the event of a personal data breach, the controller shall notify the supervisory authority competent under Article 55 without undue delay and, if possible, within a maximum of 72 hours of becoming aware of the personal data breach, without undue delay and, where possible, within a maximum of 72 hours of becoming aware of the personal data breach, unless the personal data breach would not endanger the rights and freedoms of natural persons and could not be ensured notification to the data subject.

**6.3. Explain why this has been an issue for your stakeholders?**

- The stakeholder's contract does not specify the time when the CSP must notify the stakeholder of a personal data breach, nor does it specify what information is to be contained in the notification.

**6.4. What are differences that you have encountered between stakeholders in your Member State?**

- N/A

6.5. **What are solutions to this issue? Please describe if these solutions are already implemented or potential, and whether this solution is provided by the SA or the stakeholders.**

- Document clearly the procedure for reporting a personal data breach, how long it takes for the CSP to serve the report to the stakeholder on a mandatory basis. Clearly state what information is to be included in the notification. It is possible to prepare a notification form for a personal data breach, which should be completed by the CSP and submitted to the stakeholder. This decision is provided for by Lithuanian SA, but has not yet been submitted to the stakeholder, and therefore has not been implemented.

## Part III – Actions by the SA

1. **Have you taken action (i.e. fact-finding exercises, informal contact, prior consultation, investigation) towards any of the stakeholders concerning the use of cloud-based services *prior to* launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

- N/A

2. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (E.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**

- Firstly, Lithuanian SA are considering correctives measures such as orders without the imposition of administrative fines in order to correct identified issues as soon as possible.

## Part IV – Other

1. **What is your general impression of the levels of awareness and compliance of the stakeholders you consulted concerning the use of cloud?**

- Low level of awareness concerning the use of cloud services, especially where international CSP's involved. No documented consultations with DPO, no contacting SA for advice, no documented decisions not to perform DPIA, poor level of awareness on international transfers. Depending solely on the informational provided by CSPs, not actually verifying it.

2. **Are there any other issues or topics that you would like to flag?**

- N/A

3. **Are there any leading practices of the stakeholders you have contacted that you would like to share?**

- N/A

## NL SA

Autoriteit Persoonsgegevens (Dutch DPA)

### Part I – Statistics

1. **How many stakeholders have you contacted within the following categories?**

- 3 buyers (strategic vendor managers) for the central government. The explanation of what a strategic vendor manager does is explained in question 4. For the sake of readability for the final report, however, below we refer to these strategic vendor managers as 'buyers'.

2. **How many stakeholders have you contacted within the following sectors?**

- None specific; the 3 buying departments serve several central government bodies, not from a specific sector, see question 4.

3. **If you have contacted a buyer, for which sectors does this buyer provides its services:**

- No specific sector, see question 4.

4. **If you have contacted a buyer, and if you have this information, please specify the number of stakeholders this buyer provides services for:**

- Unknown. In general, the buyers manage the relation between the Dutch Central Government and the CSPs on behalf of the organisations within the Dutch Central Government. One of the specific tasks of most buyers is to negotiate a legal framework with the CSP in order to facilitate the possible use of products and services by the organisations. The buyers do not buy products and services and do not commit to buy products and services as part of the legal framework. It is the decision of the government body to buy and/or commit to buy products and services from the CSP and as a consequence: to use cloud services.

5. **What was the initial procedural framework of your action?**

- Fact-finding + follow-up actions based on the results.

6. **How many stakeholders indicated that they use CSPs or are planning to do so in the near future (end of 2022)?**

- Not applicable, see question 4. However, we do see that most government organisations in the Netherlands use a CSP. Sometimes in the form of an on-premise solution.

7. **Of the stakeholders that use CSPs (or are planning to do so in the near future), how many use CSPs for the following functions?**

- Mainly applications for office productivity functionalities (such as administrative processes, communication and collaboration tools) and/or cloud functionalities (such as computing power, database, storage and identity & access management). However, it is not the buyers' role to determine for what purposes organisations should use these functionalities.

8. **For the following commonly identified sectors, please specify if any hyper-scalers[48] are involved (if so please name them) either because they provide the services themselves or because the services are using the infrastructures of these hyper-scalers**

[48] Hyper-scalers provide cloud services at scale. It refers usually to the big cloud providers (Google, AWS, Microsoft …) on which other services may also depend

- Central buyers or providers of IT services – Amazon, Google, Microsoft, IBM, SAP, Citrix, Oracle and several smaller CSPs.

**9. <u>How many stakeholders (*AP reads this as: buyers*) took the following actions prior to- or during the acquisition of a CSP?</u>**

- Perform a DPIA: **2 out of 3 buyers performed DPIAs or are currently conducting DPIAs. One buyer performed some DPIAs, but not for all CSPs.**

- Does the DPIA analyse transfers in details (sometimes called DTIA): **Two buyers have done an analysis on transfers or are currently conducting a DTIA, but not for all CSPs. This is because no transfer takes place or no analysis has (yet) been conducted. The Dutch SA cannot say whether all buyers have performed a DPIA/DTIA prior to the acquisition of the CSPs, also because the actual deployment is the choice of an individual government body, not of the buyer.**

- Contact the DPO for advice: **One buyer notified the DPO, but notes that it performs/commissions umbrella DPIAs, not DPIAs with respect to specific processing of personal data by a specific ministry. The scope of the umbrella DPIAs is a general data protection risk analysis for reuse by the organisations of the central Dutch Government. DPOs of different Dutch Ministries/entities can advise their specific entities falling under their supervision about the implementation or consequences of the umbrella DPIA or DTIA analysis for their individual Dutch governmental entity. Another buyer has asked the DPO for advice and the third buyer did not ask the DPO for advice.**

- Perform a general risk analysis: **The risk analysis is covered in the DPIA.**

- Contact the SA for advice: **One buyer consulted the Dutch Supervisory Authority. The outcome was used as an authoritative declaration in the negotiations with Google. It resulted in a further amended contractual document and a remediation plan as agreed with Google. The contract with Google has been signed recently, including the amended provisions as a result of the consultation.**

**10. <u>How many stakeholders (including buyers) take the following actions during the use of the CSP?</u>**

- Monitoring technical and organisational measures to ensure compliance: **One buyer states that its responsibility is to monitor the CSPs' compliance with the agreed contractual provisions in the framework agreement. For that purpose, it performs technical investigations (such as analysing data flows) on the one hand. On the other hand, it uses third party audits on the implementation of controls in the CSPs operational processes. Another buyer says that there is an intention to coordinate and facilitate the monitoring of the CSPs' compliance with the agreed contractual provisions in the framework agreement. It may perform investigations for that purpose. Whether the buyer actually does so, is unclear. The third buyer has not (yet) taken any actions.**

- In case of transfers, adopting technical and organisational measures, including supplementary measures, where needed, and monitoring if changes in the regulatory landscape occur (e.g. Schrems II). **One buyer indicates that technical and organisational measures have been proposed as mitigation for the risks as detected within the DTIA/DPIA analysis on Microsoft Teams. On the part of the CSP, certain technical measures have been announced such as the EU Data Boundary and end-2-end-encryption (E2EE) for all calls. The buyer will continue to**

**monitor all developments and guidance from the national supervisory authorities, and update the DTIA whenever that becomes necessary. For the other CSPs a DPIA/DTIA is still in progress. The second buyer has not taken any actions, since the DPIA is still ongoing for a CSP or no transfer takes place. The third buyer is on the verge of concluding an updated legal framework with a CSP and has already signed a Data Processor Agreement with references to international transfers. The buyer mentions that the CSP provides a factsheet with technical & organizational measures as mitigation for the risks from the transfer of personal data to the USA. This only concerns a limited amount of personal data, related to Website visits and Support Data. For other CSPs, there is no indication that any measures have been taken by the buyer.**

- Regular risk assessments: **All buyers have indicated that regular risk assessments are not carried out, since cloud implementation is out of their scope. Several buyers state that monitoring of law developments and required additional provisions is part of their activities. For example, one buyer monitors future legislative developments and if additional investigations or additional provisions are needed because of those developments, action will be taken by them on a general contractual level. There appear to be no set, recurring assessments activities by the buyers.**

## Part II – Substantive issues

- A more general comment from the Dutch DPA is that for the use of cloud services, there seems to be a strong focus on international transfer-issues due to Schrems II. However, there are (many) other issues that need to be addressed by public bodies in order to make legitimate use of a processor, for example further processing of personal data, the need to perform a proper (and timely) risk assessment, auditing duties post procurement, properly executing rights of data subjects and informing data subjects.

**1. <u>Contract with CSPs are 'repair work'</u>**

- Almost five years after application of the GDPR many public bodies seem to be performing assessments/DPIAs as a form of repairing already existing processing that was not fully compliant with data protection law (not only as a consequence of the Schrems II-ruling). The notion that some sort of assessment/DPIA should be included in procurement policies is rising in The Netherlands.

- Art 28 GDPR.

- Controllers are confronted with a processing of personal data that is not compliant with the GDPR. An ongoing contract has to be revised and negotiations have to take place with the CSP in order to change the terms to be compliant with the GDPR. The 'repair work' is often not beneficial for the CSP and as a consequence, the public bodies are dealing with resistance from the CSPs.

- A difference in maturity in dealing with this issue. This goes from full-fledged DPIAs with technical inspections on the data flows to mostly relying on information provided by the CSP.

- Learning from other public bodies and sharing knowledge (internationally).

**2. <u>Lack of transparency of processed data</u>**

- For customers of CSPs it can be unclear what personal data (telemetry data, data for support, etc.) is processed by the CSP and for what purposes. CSPs also tend to not want to disclose much information, because they see this as confidential information. This can make it difficult for public bodies to adequately fulfil their role as controller.

- Art 5 GDPR.

- Customers of CSPs as controllers may only process personal data in a transparent manner and only for specified and explicit purposes. Without being clear what personal data the CSP processes, customers of CSPs cannot process personal data in a manner compliant with the GDPR. For example; the customer is not able to grant a citizen (data subject) information about the processing of- or access to its personal data.

- Stakeholders do not have a complete overview of the personal data that is being processed and only rely on the general information mentioned in the contracts provided by the CSPs. In the Netherlands, a thorough traffic analysis has been conducted for some CSPs (on behalf of the central buyer) to inspect what telemetry data is collected by the CSP.

- CSPs should give clear and precise information about the personal data that is processed, including for the (specific and explicit) purposes they are processed for. In the Netherlands, some buyers seem to be successful in gaining more transparency from the CSP about this information. A controller should be well-informed by a perceived processor on the processing taking place. A processor should be able to supply this information, for instance based on current customers and his obligation stemming from article 30(2) GDPR. CSPs sometimes unjustly mention that their company trade secrets prevent them from doing so.

**3. <u>SCCs (module 2 or 3)</u>**

- One buyer has noticed a lot (if not all) CSPs are choosing module 3 of the new SCCs, the "Transfer processor to processor"- module and not the controller to processor-module (module 2).

- Art 46 (1) c GDPR.

- According to the buyer, CSPs sometimes offer the processor-to-processor SCCs instead of the controller to processor SCC as the basis for international transfer. CSPs motivate this by stating that there is an EU representation for the CSP acting as processor via whom the data is transferred outside the EU. However, the representation of a non-EU-based CSP in the EU should not be a criterion when choosing which SCC should be used. Performed factual technical checks of the actual international transfer (DTIA) clearly show that personal data are sent directly from the Dutch government to the US or third countries elsewhere (for example support data), not first through EU member states. Therefore, a controller to processor SCC should be used. The effect of wrongfully offering processor-processor SCCs instead of controller-processor SCCs is that SCCs are used that offer insufficient guaranties for the protection of personal data.

- Because of the significant power imbalance between the contractual parties in question, not every small entity shall be able to contractually agree or disagree with the standard of EU data protection once under pressure of the need for buying products and (software, cloud a.o) services. The Dutch SA has not been able to verify this statement.

- The buyer has chosen the controller to processor-module for international transfer.

4. **Insufficient (international) cooperation**

- Publicly available DPIAs, although scarce, do not seem to be widely used by public bodies.

- This leads to public bodies claiming not to know certain issues involving CSPs that they quite easily could, and thus should have known given their size and budget. The same applies for information by other government agencies such as police or intelligence agencies. Their risk assessments can be used as well. For instance, risks related to threats by foreign states looking for personal data could remain unmitigated when this information is ignored.

- Information is being shared but is sometimes focussed on a specific controller. Internationally, information is shared sparsely.

- Make DPIAs available to other public bodies and discuss effective proven ways in dealing with CSPs. The EDPB could also stimulate the publication of DPIAs from public bodies and central buyers (in the final report).

5. **Applicable terms in sub processor relationships**

- CSPs can be in a direct relationship with a public body as a supplier, but also in an indirect relationship in its role as a sub processor (for example: a CSP that provides a hosting service to a SaaS service from a different CSP). When a government body already has a contract with that CSP, the terms should also apply when the CSP acts as a sub processor, so that any 'weaker' terms are not applicable.

- Art 28 GDPR.

- In The Netherlands, specific terms are applicable with some large CSPs. As some of these CSPs can also act as a sub processor in other contracts, it is necessary that these terms are also applicable so that the public body is not dependent of any terms with a processor that may not be as detailed so that the public body can perform its role as a controller.

- This was a specific issue raised by a stakeholder, we have not identified whether this issue is also of importance at the other stakeholders.

- In the contracts with the CSPs in question a provision has been added that the terms also apply when the CSP has a contractual relationship with the public body in the role of sub processor.

## Part III – Actions by the SA

1. **Have you taken action (i.e. fact-finding exercises, informal contact, prior consultation, investigation) towards any of the stakeholders concerning the use of cloud-based services *prior to* launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

- The Dutch Ministry of Justice and Security submitted a request for prior consultation about the possible deployment of Google G Suite Enterprise/Google Workspace by Dutch governmental organisations. We advised against the use of Workspace and Workspace for Education by both parties, because the submitted DPIAs raised fundamental questions about, amongst others, the lack of transparency and the role of processor- and controllership. With our advice, the

negotiating parties reached an agreement with Google. In the explanatory letter sent to the Parliament, the Ministry has stated that all high-risks are mitigated to such an extent that they no longer classify as 'high'.

2. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (E.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**

- We keep (informal) contacts with one of the buyers and the CIO department of the central government (CIO Rijk). This is mainly to be updated (on a high level) about the negotiations with CSPs and to retrieve information on the overarching issues regarding the acquisition of CSPs. We also keep contacts with CIO Rijk about the cloud strategy from the Dutch central government and the DPOs, to update them about our findings. We might also be sending a guidance letter towards the central government about the acquisition of CSPs. This could contain some brief feedback on the findings that we have done as part of this coordinated action and also some recommendations towards the future.

## Part IV – Other

1. **What is your general impression of the levels of awareness and compliance of the stakeholders you consulted concerning the use of cloud?**

- It is hard to give a general impression, as we have seen that the level varies greatly between the 3 buyers that we have consulted. For one buyer the level appears to be very high. We see that a lot of time and resources (including by consulting external organisations) are invested to raise the compliance level in contracts with the large CSPs; this is not a maturity level that every organisation can achieve (on its own). On the other hand, we have also seen a buyer that gave very vague information and does not seem to have the expertise and resources available to achieve a high level of awareness/compliance. Fortunately, we do see that a certain level of cooperation is taking place between the buyers (and DPOs), which raises the overall level.

2. **Are there any other issues or topics that you would like to flag?**

- Cooperation is key in negotiating contracts with large CSPs; in the Netherlands, buying organisations are taking a more important role (also in the educational sector). We believe that SAs can contribute to the overall level of compliance by encouraging this type of cooperation. This cooperation should take place on both on a national level (e.g. within a certain sector) and on an international level (publishing DPIAs and learning from contractual agreements made by other parties).

- We would also like to quote the following answer we have received from one of the buyers regarding the experiences performing a DPIA:

> *"A positive experience with performing a DPIA is the leverage which is created if data protection risks are identified. We clearly benefit from the harmonisation of European (privacy) laws, since the risks identified in the DPIA can be applied by all European organisations that use the services of the same CSP. CSPs are aware that assessed risks are potentially blocking their business in the EU. A negotiation about the assessed risk-mitigation also opens the door for related issues like liability in case of breaching the DPA. For the CSPs, the negotiations with [buyer] also offer added value, because they benefit from input on*

*specific mitigation measures, and by being able to confidentially discuss obstacles and timeframes to implement such mitigation measures.*

*Negative experiences are the huge investments in technical, legal and CSP management capacity. [Buyer] is able to organise this on a central government level, but it still requires a lot even from a central government organised team. The financial investments are also huge, because external experts are needed during the whole process of investigation, negotiations and contracting with CSPs, together with at least 3 or more civil servants. Added to this is the relatively new requirement of performing a DTIA, for which even more capacity is needed. The results of [buyers] work are only applicable to civil servants, related (external) contract workers and Dutch persons who are interacting with employees under a central government license. Private sector organisations and consumers/citizens are not covered by the results of [buyers] work. Because the negotiated legal frameworks need proper management, additional investments (e.g. technical verification, audits, DPIA's) are required on an ongoing basis."*

- The lack of a clear cloud national strategy gives room for public bodies to make their own individual decisions. Decisions including why, when and how a CSP is being contracted. While, in individual cases, it can be inefficient to start thinking about a private cloud, this can become much more feasible from a countrywide perspective. A countrywide cloud strategy could include a timeline for development of a national, or European, cloud infrastructure (gradually) developing from an IaaS to a SaaS-solution. This will also impact the decision on the necessity of choosing a non-EU CSP in the years to come.

**3. <u>Are there any leading practices of the stakeholders you have contacted that you would like to share?</u>**

- Yes, we would like to share the following best practices from one of the buyers:
    - Conducting 'umbrella' DPIAs and DTIAs in which the 'default' processing of the cloud platform is technically investigated in several defined use cases that (governmental) organisations can use for their own assessment.
    - Publishing DPIAs and DTIAs on a publicly accessible website.
    - An approach that contractually guarantees the processing of personal data only on documented instructions. Furthermore, all possible purposes are explicitly authorized in the documented instructions. These purposes are included to ensure that processing does not go beyond what is necessary to deliver the service, keep the services secure and up to date.
    - With regards to purpose limitation, the buyer takes the following approach:
        - There is a limitative list of authorized purposes for which the processor may process personal data, for example: providing the service, keeping it up to date and secure.
        - The buyer explicitly authorises the CSP to 'further' process some personal data for narrowly defined purposes. These purposes are defined in an exhaustive list in the (amended) data processing agreement, which is part of the legal framework. The purposes are related to legitimate business purposes for which the CSP necessarily has to act as the sole controller, such as invoicing, accounting, fraud detection and technical infrastructure forecasting.

    - To further limit processing of personal data outside the scope of authorized purposes, the instructions include certain prohibited purposes. This means that the CSP for example may not use personal data for profiling, advertising or analytics. This approach is an extra measure to ensure that a CSP cannot use the data for all things he renders necessary as a controller.

- Initially, the DPIAs on both Microsoft and Google services concluded that factually the organisations and the CSP were joint controllers, and flagged the lack of control over the data processing (due to the lack of transparency and lack of a joint controller agreement) as a high risk. After the negotiations about mitigating measures, the CSPs are no longer joint controllers.

- Verification of the CSP's compliance with the agreed legal framework is also managed by the buyer. This means that, with regard to the data processing agreement, the buyer selects certain services to audit in a technical way (technical verification against contractual provisions) combined with audits with respect to the CSP internal processes (and the controls thereof).

- The processor is allowed to engage a sub processor. For the engagement of a sub processor that is related to essential or core services, the notification of engagement is sent substantially sooner, as it is possible that the sub processor will gain access to customer content data.

- The buyer routinely carries out technical verification analyses with the assistance of qualified third parties. For example, the buyer verifies whether services indeed comply with a committed security level. Moreover, specific security measures and frameworks are specified in the legal framework. It should be noted that the customer in such a scenario is largely dependent on the cooperation on the part of the vendor. This is of great importance, as there are no other means to verify any obligation without adequate cooperation of the vendor. The buyer always includes specific extensive audit provisions in the legal framework, to prevent possible conflicts when verifying compliance with external auditors.

# PT SA

## Comissão Nacional de Proteção de Dados – CNPD - Portugal

### Part I – Statistics

1. **How many stakeholders have you contacted within the following categories?**

- Ministry of the central government
- Independent public body of the central government **(3)**
- Buyer for the central government
- Publicly-owned company acting as a processor for several central public bodies
- Ministry of the regional government
- Independent public body of the regional government
- Buyer for the regional government
- Publicly-owned company acting as a processor for several regional public bodies
- Other, please specify: public buyer for public health sector **(1)**

2. **How many stakeholders have you contacted within the following sectors?**

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government **(2)**
- Economic affairs
- Education
- Finance
- Health **(1)**
- Infrastructure
- Employment
- Justice
- Tax
- Other, please specify: social security **(1)**

3. **If you have contacted a buyer, for which sectors does this buyer provides its services:**

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government
- Economic affairs
- Education
- Finance
- Health **(1)**
- Infrastructure
- Employment
- Justice
- Tax
- No specific sector
- Other, please specify
-

4. **If you have contacted a buyer, and if you have this information, please specify the number of stakeholders this buyer provides services for:**

- 120.000 in 1900 .locations

5. **What was the initial procedural framework of your action?**

- Fact finding
- Fact finding + determining follow-up action based on the results
- New investigation[49] **X**
- Ongoing investigation

6. **How many stakeholders indicated that they use CSPs or are planning to do so in the near future (end of 2022)?**

- All of the stakeholders investigated: 4

7. **Of the stakeholders that use CSPs (or are planning to do so in the near future), how many use CSPs for the following functions?**

- Internal organisation (office suites, internal communication, HR, etc.) - **(4)**
- Exercise of public functions (services to citizens, processing citizen's data, etc.) – **(1)**

8. For the following commonly identified sectors, please specify if any hyper-scalers50 are involved (if so please name them) either because they provide the services themselves or because the services are using the infrastructures of these hyper-scalers: **No**

- Health
- Finance
- Tax
- Education
- Central buyers or providers of IT services

9. **How many stakeholders took the following actions prior to- or during the acquisition of a CSP?**

- Perform a DPIA **(0)**
- Does the DPIA analyse transfers in details (sometimes called DTIA) **(0)**
- Contact the DPO for advice **(2)**
- Perform a general risk analysis **(3)**
- Contact the SA for advice **(0)**

10. **How many stakeholders (including buyers) take the following actions during the use of the CSP?**

- Monitoring technical and organisational measures to ensure compliance: **none**
- In case of transfers, adopting technical and organisational measures, including supplementary measures, where needed, and monitoring if changes in the regulatory landscape occur (e.g. Schrems II): **none**
- Regular risk assessments: **none**

## Part II – Substantive issues

1. **No direct contract with the CSP and no negotiation of the terms**

- The absence of a direct contract with the CSP is a common issue to all stakeholders, and it seems that stems from the way the most known CSP conduct their business. This is a problem, because there is no possibility of negotiating the terms of the contract, in particular taking advantage of a

[49] making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred

[50] Hyper-scalers provide cloud services at scale. It refers usually to the big cloud providers (Google, AWS, Microsoft …) on which other services may also depend

broad expected use of the services, or of the fact that it is a public body directly linked to the central government with a higher negotiating power. In addition, it becomes more difficult to have tailor-made rules covering the contract and providing an adequate reply to certain legal requirements. Somehow, this limits the choice of a processor that offers guarantees, as required by Article 28(1) GDPR. There is a clear inversion of roles, when the processor is not in a position to choose and to instruct the (sub) processor. The processor is just an intermediary and it only artificially performs the tasks envisaged by the GDPR and entrusted by the controllers.

- The solution is to find CSPs that are willing to negotiate directly and that submit themselves to the public procurements for their services, without using proxy (national) companies to make the contracts.

- Furthermore, some controllers rely on the terms of the contract with the intermediary companies (processors) to demand certain legal conditions to meet data protection requirements (obligation of result) that objectively cannot be ensured by those processors, as they are in no position to give further instructions to the sub(processors) that actually provide the cloud services. This having into account that the CSPs at stake are the so-called Internet giants. It is indeed a false indication of compliance.

**2. No clear allocation of roles among the public bodies**

- The public bodies launching the procurement for cloud services and entering into contracts are not, in some cases, the actual controllers. Some IT public institutes assume the role of controllers, when making the decisions on the means and on the purposes of the processing without consulting the 'owners of the data', i.e. who by virtue of their legal competences are the effective controllers and employers of the human resources using the cloud services. Even if in some situations a joint controllership would be applicable and the most suitable solution, such arrangement is not in place pursuant Article 26 GDPR. This excludes the effective controllers of the decision-making process and, thus, of their responsibilities. The pandemic crisis led to a quick recourse to cloud services because of teleworking, without contemplating all the pros and cons of such solutions. Furthermore, with the confinement, there was an increased need of public services are available remotely and online by citizens.

**3. Lack of DPIA**

- None of the stakeholders carried out a DPIA to assess the impact of the choice of having cloud services and the extent of the use of such services.

- This is in breach of Article 35 (1) GDPR. This shows that controllers are not fully aware of their data protection obligations. Moreover, the lack of DPIA did not allow the identification of risks and the adoption of appropriate measures to mitigate such risks or to decide on alternative ways to get the needed services. Two stakeholders performed some risk analysis, in very general terms, what did not permit to have a thorough overview of the essentials. In addition, data protection officers were not properly involved from the outset in the projects; thus, they did not have the opportunity to convey their advice to the controller.

**4. Failures in the contract with processor**

- The DPA identified failures in the data processing agreements required by Article 28 GDPR. The controllers entered into contracts with (intermediary) processors, but not all legal conditions were met. The Service Level Agreement (SLA) was in fact the core of the contract. No negotiating terms, as explained in Issue 1, or imposed limitations on data processing. However, all contracts contain

reversibility/termination control clauses. Only one stakeholder incorporated clauses on data breaches.

- Another relevant aspect is the fact that the insertion of some requirements in the contract (like, location of the data) are not implemented in practice or monitored whatsoever by the stakeholder, since the (intermediary) processor is not in a position to ensure the compliance with this term of the contract. On the other hand, the stakeholder (controller) does not take any other steps to verify or guarantee that the data is indeed in the EU and that is not acceded by third country authorities. This is connected with the following issue 4.

5. **Insufficient assessment towards the requirements on international transfers**

- The stakeholders show to have insufficient awareness of the legal framework on international transfers, in particular after the Schrems II judgement. Some stakeholders managed to secure in the contracts with the (intermediary) processor the condition that the personal data stays within the EU. But at the same time, they accept standard contractual clauses as a valid mechanism for international transfers. No assessment was made on the factual conditions of the data processing, including transfers to third countries (e.g. via telemetry or via direct governmental access to data centres located in the EU). Misinterpretation that a simple clause in the contract requiring the data to be located in Portugal or within the EU is enough to ensure that data is no further transferred. Therefore, no assessment of the third country is done or supplementary measures requested or adopted.

6. **Lack of awareness in relation to telemetry and diagnosis data**

- The stakeholders were not aware of the processing of data for purposes of telemetry and of the respective legal obligations. No requirements were made or negotiated, in order to apply the principle of data minimisation (Article 5(1) (c) GDPR); the principle of data protection by design and by default (Article 25); security measures (article 32). It was evident that some of this data was used by the stakeholders, but in some limited extent, in particular in what audit logs are concerned. In general, this kind of data is not perceived as personal data subject to GDPR requirements by all stakeholders.

7. **Lack of monitoring of compliance**

- The stakeholders do not perform any kind of check on compliance or monitoring of the actions carried out by processors, in clear breach of Article 28. This is a common conclusion from the investigation on the four stakeholders. There are no procedures in place in case of data breaches, especially because the cloud solutions are seen as more secure solutions than other alternatives. Yet some cyberattacks already known target or explore security breaches in the processors that disclose users' credentials and enable an entry into the organisations and get access to their infrastructures.

## Part III – Actions by the SA

1. **Have you taken action (i.e. fact-finding exercises, informal contact, prior consultation, investigation) towards any of the stakeholders concerning the use of cloud-based services *prior to* launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

- No. The Coordinated enforcement action was the starting point for the inspection of 4 stakeholders at national level.

2. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (E.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**

- No decision was taken so far, as the inspection reports are yet to be finalised. Then, the data protection authority will issue a decision, which cannot be anticipated at this point; however, the minimum outcome will be recommendations to the stakeholders. But based on similar situations, most likely some corrective measures will be applied.

## Part IV – Other

1. **What is your general impression of the levels of awareness and compliance of the stakeholders you consulted concerning the use of cloud?**

- In general, it is our impression that there was a certain level of awareness on the risks associated with cloud services, in particular related to international transfers, as this has been an issue with some media coverage after the Schrems II and the DPA decisions; hence, the requirement on the location of data within the EU. However, in practical terms, the solutions adopted are clearly insufficient to tackle the issue. In addition, under the pressure of finding options during the pandemic crisis and the need to address teleworking and online access by citizens to public services with urgency, no prior risks assessments (such as DPIAs) were carried out or the high involvement of DPOs. It could also be underlined that the adoption of cloud services solutions is a result of public bodies being understaff in IT experts. The cloud solutions require much less in-house manpower to manage the infrastructures.

2. **Are there any other issues or topics that you would like to flag?**

- The fact that there is no direct contract or negotiation with the CSP (in case of big multinational companies) hinders the proper compliance of Article 28 and the other GDPR obligations.

- It should be highlighted though that the use of CSP is not applicable to the core activities of the public bodies, i.e. not involving data processing of a large universe of data subjects. The stakeholders concern have their own data centres and infrastructures, where the data is stored, what is very positive. The cloud services mostly used relate to active directories, email functionalities, videoconference and office productivity tools.

- Conversely, there is no specific training to staff on how to use these tools appropriately, in particular preventing from processing personal data of citizens using the cloud storage capabilities, within the daily activities.

3. **Are there any leading practices of the stakeholders you have contacted that you would like to share?**

- No

# SE SA

## National Report: Swedish SA

### Part I – Statistics

**1. <u>Which stakeholders have you contacted under the coordinated action?</u>**

- The Swedish Tax Agency
- Enforcement Authority (government agency that deals with debts)
- The Swedish Social Insurance Agency
- The Swedish Pensions Agency
- The Swedish Companies Registration Office
- The Swedish Public Employment Service
- The Swedish Board of Student Finance
- The Agency for Digital Government
- The Swedish Civil Contingencies Agency
- The Swedish Transport Administration
- The Swedish Mapping, cadastral and land registration authority

**2. <u>How many stakeholders have you contacted within the following categories?</u>**

- Ministry of the central government: **0**
- Independent public body of the central government: **11**
- Buyer for the central government: **0**
- Publicly-owned company acting as a processor for several central public bodies: **0**
- Ministry of the regional government: **0**
- Independent public body of the regional government: **0**
- Buyer for the regional government: **0**
- Publicly-owned company acting as a processor for several regional public bodies: **0**
- Other, please specify

**3. <u>How many stakeholders have you contacted within the following sectors?</u>**

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government: **1**
- Economic affairs
- Education
- Finance: **3**
- Health
- Infrastructure: **3**
- Employment: **1**
- Justice
- Tax: **1**
- Other, please specify: **3**

**4. <u>If you have contacted a buyer, for which sectors does this buyer provides its services?</u>**

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government
- Economic affairs
- Education

- Finance
- Health
- Infrastructure
- Employment
- Justice
- Tax
- No specific sector
- Other, please specify

5. **If you have contacted a buyer, please specify the number of stakeholders this buyer provides services for**

6. **What was the initial procedural framework of your action?**
- Fact finding **X**
- Fact finding + determining follow-up action based on the results
- New investigation
- Ongoing investigation

7. **How many stakeholders indicated that they use CSPs or are planning to do so in the near future (end of 2022)?**
- We received 7 answers, all of them said they use CSPs.

8. **Of the stakeholders that use CSPs (or are planning to do so in the near future), how many use CSPs for the following functions?**
- Internal organisation (office suites, internal communication, HR, etc.)
- Exercise of public functions (services to citizens, processing citizen's data, etc.)

- **Answer:** Answers were not very clear, but it seems like all of them are mainly using CSPs for internal organisation.

9. **For the following commonly identified sectors, please specify if any hyper-scalers are involved (if so please name them)**
- Health
- Finance
- Tax
- Education
- Central buyers or providers of IT services

10. **How many stakeholders took the following actions prior to- or during the acquisition of a CSP?**
- Perform a DPIA: **6/7 (However, they do not seem to be performing DPIAs for every single acquisition, but when a DPIA is required.)**
- Does the DPIA analyses transfers in details (sometimes called DTIA): **7/7**
- Perform a general risk analysis: **7/7**
- Contact the DPO for advice: **7/7**
- Contact the SA for advice: **0/7**

11. **How many stakeholders (including buyers) take the following actions during the use of the CSP?**
- Monitoring technical and organisational measures to ensure compliance: **6/7**

- In case of transfers, adopting technical and organisational measures, including supplementary measures, where needed, and monitoring if changes in the regulatory landscape occur (e.g. Schrems II): **4/7**
- Regular risk assessments: **4/7**

## Part II – Substantive issues

- **Name the issue and briefly describe the main issue(s) identified.**
- **Which provision(s) of the GDPR (or national laws) does this concern?**
- **Explain why this has been an issue for your stakeholders?**
- **What are differences that you have encountered between stakeholders in your Member State?**
- **What are solutions to this issue? Please describe if these solutions are already implemented or potential, and whether this solution is provided by the SA or the stakeholders.**

**1. <u>Contract with the CSP</u>**

- Answers regarding the roles differs between different stakeholders, some (4/7) say the authority is the controller and the CSP is processor, some answers are really short and one answer indicates that there is a joint controllership with the CSP.
- Art 24, 26
- The answers do not really clarify.
- More guidance and maybe inspections regarding the responsibility for organisations when using CSPs.

**2. <u>International transfers and access by foreign public authorities</u>**

- 4/7 authorities do not really answer the question about if personal data is being transferred to third countries. 3/7 seem to be transferring data to some extent or at least in a few cases. We can assume that transfers are being made at least occasionally even in the cases where they did not answer. However, regarding which tool of transfer the transfers are based on, 4/7 did not answer and only 1/ mentioned SSCs and 1/7 mentioned art 49. Conclusion in transfers are being made without an applicable tool of transfer.
- Art 44-49
- Doesn't say but probably because the difficulty to use US CSPs and how to deal with that situation, and the difficulty to perform TIAs.
- Larger problems for smaller organisations who do not have the financial resources to hire staff who have deeper knowledge about both technical and legal issues, also harder for them to negotiate with CSPs.
- Guidance is always valuable, maybe inspections are more efficient when it comes to making the CSPs change and create services that are compliant with the GDPR.

**3. <u>Telemetry data</u>**

- Only 1/7 authorities are answering that they do investigate whether telemetry data is being collected by the CSP. 6/7 are not answering or answer that they do not know. Follow up questions are not really being answered, or the answer is that they don't' know.
- Responsibility issue, art 24.
- Doesn't say but there is probably not very much awareness about collection of this kind of data, authorities are probably focusing mainly on 'direct' personal data.
- Hard to say, there seem to be a lack of awareness among all the authorities in this case.
- Maybe more guidance as a start, since the stakeholders seem to lack basic knowledge about this.

4. **Compliance**

- 6/7 stakeholders claim they do monitor the implemented technical and organisational measures, but during which circumstances they do that differs. However, only 3/6 monitor if the CSP perform risk assessments.
- Art 24, 32
- Does not say but monitoring risk assessments probably demands a higher level of awareness by the controller, than monitoring TOMs. Some stakeholders probably have not reached that level (yet).
- Hard to say, but authorities with more experience in using CSPs are probably most likely to have knowledge about the need to monitor risk assessments.
- Maybe guidance as a start, some stakeholders seem to lack awareness about this, but inspections might be needed as well further on.

## Part III – Actions by the SA

1. **Have you taken action (i.e. fact-finding exercises, informal contact, prior consultation, investigation) towards any of the stakeholders concerning the use of cloud-based services *prior to* launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

- Answer: No.

2. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (E.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**

- Answer: We have written a report regarding the national investigation in November 2022.

## Part IV – Other

1. **What is your general impression of the levels of awareness and compliance of the stakeholders you consulted concerning the use of cloud?**

- Answer: Pretty good awareness regarding the process for acquisition, regarding the international transfers and processing of telemetry data not so good. We did however send the questionnaire to big authorities who we believe have a lot of experience in using cloud-based services, the level of awareness is probably lower among authorities in general in Sweden.

# SI SA

## Slovenian SA (Information Commissioner of the Republic of Slovenia)

### Part I – Statistics

1. **How many stakeholders have you contacted within the following categories?**

- Ministry of the central government: **1**
- Independent public body of the central government: **0**
- Buyer for the central government: **0**
- Publicly-owned company acting as a processor for several central public bodies: **0**
- Ministry of the regional government: **0**
- Independent public body of the regional government: **0**
- Buyer for the regional government: **0**
- Publicly-owned company acting as a processor for several regional public bodies: **0**
- Other, please specify: **3 public research institutes**

2. **How many stakeholders have you contacted within the following sectors?**

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government
- Economic affairs
- Education: **4**
- Finance
- Health
- Infrastructure
- Employment
- Justice
- Tax
- Other, please specify

3. **If you have contacted a buyer, for which sectors does this buyer provides its services:**

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government
- Economic affairs
- Education
- Finance
- Health
- Infrastructure
- Employment
- Justice
- Tax
- No specific sector
- Other, please specify
- Not applicable

4. **If you have contacted a buyer, and if you have this information, please specify the number of stakeholders this buyer provides services for:**

- 5

5. **What was the initial procedural framework of your action?**

- Fact finding
- Fact finding + determining follow-up action based on the results
- New investigation[51]
- Ongoing investigation

6. **How many stakeholders indicated that they use CSPs or are planning to do so in the near future (end of 2022)?**

- 1

7. **Of the stakeholders that use CSPs (or are planning to do so in the near future), how many use CSPs for the following functions?**

- Internal organisation (office suites, internal communication, HR, etc.) : **1**
- Exercise of public functions (services to citizens, processing citizen's data, etc.): **1**

8. **For the following commonly identified sectors, please specify if any hyper-scalers[52] are involved (if so please name them) either because they provide the services themselves or because the services are using the infrastructures of these hyper-scalers**

- Health
- Finance
- Tax
- Education: Microsoft 356
- Central buyers or providers of IT services

9. **How many stakeholders took the following actions prior to- or during the acquisition of a CSP?**

- Perform a DPIA: **0**
- Does the DPIA analyse transfers in details (sometimes called DTIA): **0**
- Contact the DPO for advice: **0**
- Perform a general risk analysis: **0**
- Contact the SA for advice: **0**

10. **How many stakeholders (including buyers) take the following actions during the use of the CSP?**

- Monitoring technical and organisational measures to ensure compliance: **0**
- In case of transfers, adopting technical and organisational measures, including supplementary measures, where needed, and monitoring if changes in the regulatory landscape occur (e.g. Schrems II) : **0**
- Regular risk assessments: **0**

## Part II – Substantive issues

1. **LACK OF CONDUCTING DPIA [53]**

[51] making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred

[52] Hyper-scalers provide cloud services at scale. It refers usually to the big cloud providers (Google, AWS, Microsoft …) on which other services may also depend

[53] the issue identified is based solely on the response of one questionnaire since only one participant stated that they use a CSP

- Despite the many risks that the use of cloud services in the public sector has on the protection of personal data, we gathered from the responses of the participating stakeholder that uses a CSP that a DPIA has not been conducted, neither before the intended processing itself, nor in the process of stipulating contractual provisions.

- Article 35 and 36 GDPR; relevant recitals of the GDPR: (75), (76), (77), (84), (90), (91), (92), (93), (95).

- Due to the lack of DPIA being conducted by the controller, we see challenges in terms of controller not fully understanding all the obligations regarding personal data protection and the importance of DPIA as a tool to mitigate various personal data processing risks.

- One stakeholder stated that they use a CSP and has not conducted DPIA.

- SI SA has already published general guidelines on the implementation and importance of data protection impact assessment (https://www.ip-rs.si/prirocniki_smernice/Smernice_o_ocenah_ucinka.pdf), which will be reviewed in more detail and supplemented according to the specifics of the processing resulting from the use of cloud services in the public sector. In addition, in accordance with the (national or EDPB) findings, targeted trainings on this topic could additionally be conducted, focused on a clearly defined circle of organizations in the public sector that implement or use such services in their work.

**2. LACK OF SUFFICIENT GUARANTEES FORSEEN IN REGARDS TO ENSURING APPROPRIATE TECHNICAL AND ORGANISATIONAL MEASURES**

**AND**

**3. MONITORING OF THE IMPLEMENTED TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING SECURITY MEASURES OF THE CSPS[54]**

- Controllers often do not have all the information about how a certain cloud provider ensures some essential elements of personal data security, such as the traceability of processing, the deletion of personal data after the purpose of processing has been fulfilled, and information about the actual locations of personal data etc. In such situations, it is difficult for personal data controllers to carry out adequate risk analysis before deciding to use these cloud services. Based on the response from one stakeholder that uses a CSP we identified a lack of sufficient guarantees in relation to assurances about (adequate security, technical and organisational measures that are being implemented by the cloud service provider.

- Article 32 GDPR; Article 24 & 25 of Personal Data Protection Act (ZVOP-1);

- Based on the response of one stakeholders, we note a lack of implementation of technical or organizational measures to mitigate risks and establish adequate safeguards prior to the processing carried out when using cloud service providers. Additionally there is no monitoring mechanism provided or used by the controllers. One stakeholder states that they only perform the measure of sporadic inquiry about the physical location of the data.

- No substantial differences have been noticed.

[54] the issue identified is based solely on the response of one questionnaire since only one participant stated that they use a CSP

- Given the lack of basic knowledge in the field of personal data protection, alongside the diversity and complexity of the risks that the use of this type of technology has on the protection of personal data, it would be necessary to further educate the relevant public and implement various preventive mechanisms (such as additional guidelines, training…), which would encourage the awareness of these controllers and ensure greater compliance in this area.

**4. UNCLEAR ROLE OF THE PARTIES[55]**

- Controllers in general often accept the general conditions of the use of services, where the controller of personal data is often a party with less bargaining power, who can usually only accept or reject the general conditions of the use of services submitted to him by the provider of cloud computing services, even though the controller of personal data is the one who determines the purposes, circumstances and means of processing and the required level of protection of personal data. Due to the disproportionate balance of power it is crucial that the there is a clear determination of roles done by the controller and by the processor. The controller must adequately establish its role in the processing activities and its relation to the cloud services provider, while the contract must specify the controls regarding the processing of the processor and specify the risk mitigating measures within the contract;

- Articles 24, 26 - 29 GDPR, Article 11 Personal Data Protection Act (ZVOP-1);

- It follows from the responses of the stakeholder that uses the CSP that they are not aware of the content of the contract, which was accepted on their behalf by the central buyer of the cloud services of the specific provider, nor that this contract contained any essential provisions on ensuring compliance of personal data processing with relevant regulations in the field of personal data protection.

- No substantial differences have been noticed.

- Given the controller's lack of basic knowledge in the field of personal data protection, additional training might be necessary. In addition, it should be noted that the participating stakeholder did not involve a DPO when determining or accepting the relevant contract with the CSP. With that in mind, the role of the DPO when determining such processing activities based on a contract should be emphasized.

**5. LACK OF AWARENESS ON INTERNATIONAL PERSONAL DATA TRANSFERS [56]**

- Specific difficulties in ensuring the expected level of protection of personal data also arise from the related issues of exporting personal data to third countries that (do not) provide the same levels of personal data protection as the home jurisdiction. This especially applies when the personal data that is being transferred is by a public sector organisation and/or large in volume.

- Chapter V. of GDPR, Article 63-71 ZVOP-1.

[55] the issue identified is based solely on the response of one questionnaire since only one participant stated that they use a CSP

[56] the issue identified is based solely on the response of one questionnaire since only one participant stated that they use a CSP

- Since the answers were quite limited in scope and in its content, it can be deducted that there is a lack of awareness on the problematics and obligations of using a provider where the rules of international persona data transfer applies.

- No substantial differences have been noticed.

- SI SA has already written quite a vast number of non-binding opinions and included the topic of international data transfers in many of our general guidelines. Based on results we will analyse whether there is a need for a specific training, promotion of our guidelines and/ or other preventive mechanism is necessary.

## Part III – Actions by the SA

1. **Have you taken action (i.e. fact-finding exercises, informal contact, prior consultation, investigation) towards any of the stakeholders concerning the use of cloud-based services *prior to* launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

- Before the implementation of our joint coordinated action, SI SA issued a number of non-binding opinions on the obligations of controllers regarding their use of cloud services. We emphasized the importance of transparency and available information to individuals, the controller's responsibility for ensuring adequate technical and organizational measures for data security, and the importance of conducting the data protection impact assessment to evaluate the effects on the protection of personal data. In addition to the aforementioned actions above, we also issued general guidelines on cloud computing, where we first defined the main features and concepts of cloud computing and described in more detail the obligations of controllers in relation to the export of personal data to third countries, adequacy of contractual provisions, security of personal data processing, etc. As part of the mentioned guidelines, we have also created a checklist for checking the controller's compliance when using cloud-computing services concerning personal data protection requirements.

2. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (E.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing)**

- We will continue to issue non-binding opinions and guidelines on this topic by taking into the account the findings of this coordinated action, while also emphasizing the importance of a consistent and careful approach to the introduction and use of cloud service provides in the public sector. We will consider potential updates to our (already existing) guidelines on cloud computing. Based on the findings we will also consider if further enforcement measures will be applied.

## Part IV – Other

1. **What is your general impression of the levels of awareness and compliance of the stakeholders you consulted concerning the use of cloud?**

- The stakeholders to whom we addressed the respective questionnaire demonstrated limited knowledge of both understanding (i) what cloud services are (ii) their obligations in connection

with the protection of personal data arising from their use. Based on four obtained questionnaires, we received an answer of only one stakeholder where they confirmed the use the cloud service provider both for organizational work within the organization and for the implementation of their public function. The other stakeholders confirmed to us that they do not use cloud services, outside of the use of providers such as Zoom and Cisco, although some use for example Google Analytics on their website. In conclusion, we also note the lack of both the inclusion of DPOs in the process of adopting contractual provisions as well as the lack of conducting the DPIA, as a preventive tool in identifying the risks that a concrete processing may have on the right to the protection of personal data. In addition, it can be deduced from the answers that the stakeholders are rather unaware of the problems and risks of using such technologies for the rights of individuals and the problem of the transfer of personal data to third countries.

2. **Are there any other issues or topics that you would like to flag?**

3. **Are there any leading practices of the stakeholders you have contacted that you would like to share?**

# SK SA

## Part I – Statistics

1. **How many stakeholders have you contacted within the following categories?**

- Ministry of the central government: **2**
- Independent public body of the central government: **3**
- Buyer for the central government
- Publicly-owned company acting as a processor for several central public bodies
- Ministry of the regional government
- Independent public body of the regional government
- Buyer for the regional government
- Publicly-owned company acting as a processor for several regional public bodies
- Other, please specify

2. **How many stakeholders have you contacted within the following sectors?**

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government: **1**
- Economic affairs
- Education
- Finance: **1**
- Health
- Infrastructure: **1**
- Employment
- Justice
- Tax
- Other, please specify – audit, statistics

3. **If you have contacted a buyer, for which sectors does this buyer provides its services:**

- Agriculture
- Defence
- Digitalisation of the Public Administration/e-Government**: Probably yes, the Ministry negotiates framework documentation and each stakeholder must conclude its own contract using this framework documentation. (The word "probably" is just solely for the reason that in order to expressly confirm the factual situation, more evidence shall be gathered (as we did not exactly ask for this question in the questionnaires).**
- Economic affairs
- Education
- Finance
- Health
- Infrastructure
- Employment
- Justice
- Tax
- No specific sector
- Other, please specify

4. **<u>If you have contacted a buyer, and if you have this information, please specify the number of stakeholders this buyer provides services for:</u>**

- We have not demanded for this information.

5. **<u>What was the initial procedural framework of your action?</u>**

- Fact finding
- **Fact finding + determining follow-up action based on the results**
- New investigation[57]
- Ongoing investigation

6. **<u>How many stakeholders indicated that they use CSPs or are planning to do so in the near future (end of 2022)?</u>**

- 5

7. **<u>Of the stakeholders that use CSPs (or are planning to do so in the near future), how many use CSPs for the following functions?</u>**

- Internal organisation (office suites, internal communication, HR, etc.): **5**
- Exercise of public functions (services to citizens, processing citizen's data, etc.): **3**

8. **<u>For the following commonly identified sectors, please specify if any hyper-scalers[58] are involved (if so please name them) either because they provide the services themselves or because the services are using the infrastructures of these hyper-scalers</u>**

- Health
- Finance: **1**
- Tax
- Education
- Central buyers or providers of IT services

9. <u>How many stakeholders took the following actions prior to- or during the acquisition of a CSP?</u>

- Perform a DPIA
- Does the DPIA analyse transfers in details (sometimes called DTIA)
- Contact the DPO for advice
- Perform a general risk analysis
- Contact the SA for advice

- Answer: 0

10. **<u>How many stakeholders (including buyers) take the following actions during the use of the CSP?</u>**

- Monitoring technical and organisational measures to ensure compliance
- In case of transfers, adopting technical and organisational measures, including supplementary measures, where needed, and monitoring if changes in the regulatory landscape occur (e.g. Schrems II).
- Regular risk assessments

[57] making use of the SAs formal investigatory powers in order to determine whether an infringement has occurred

[58] Hyper-scalers provide cloud services at scale. It refers usually to the big cloud providers (Google, AWS, Microsoft …) on which other services may also depend

- Answer: 0

## Part II – Substantive issues

**1. <u>At pre-contractual phase</u>**

- Based on the answers provided in the questionnaires, we noticed lack of knowledge about the fact that that the services used by stakeholders are identified as cloud services. They seem not to take into account GDPR rules not only during pre-contractual phase but also during the implementation phase. Another principal issue resulting from the answers is that the answering body did not even understand technology or law at stake. Consequently, answers provided were not factually correct – people with technical background do not understand legal questions, and vice-versa, people with legal background answered the questionnaire incorrectly, but in line with what the GDPR is supposed to require (however, the practice is obviously different).

- N/A

- We have received contradicting answers, Stakeholder responsible for the framework of contractual relationships for public bodies declared that they use only one type of cloud service and other Stakeholder claimed that they are using other type of cloud service but contractual relationships are procured by the former Stakeholder and that they do not have power to change the contractual relationship.

- We have found out that the level of knowledge and compliance practice with data protection rules are low. We have not received any answer from the concerned public body that would obviously provide evidence that the GDPR rules are taken into account at pre-contractual phase. The main difference is that some stakeholders said that they use only one type of service cloud provider. However, we did not receive convincing information that would confirm that the GDPR rules are taken into account prior to conclusion of contractual relationship even with the one cloud provider. In one case, the stakeholder stated that they are working on the amendments to the contract which will cover data protection or that there is no controller-processor contract and only the business contract presuppose conclusion of controller-processor contract which has not been concluded yet.

- With regard to the basic knowledge about the GDPR requirements of the stakeholders involved in the questionnaire, we are considering how to improve data protection knowledge within their employees. Currently, we will propose stakeholders to organise trainings about the cloud related topics targeting data protection obligations, which should be provided by their Data Protection Officers and send evidence about this specific trainings to SA. Another solution, which we plan to initiate, based on the analysed questionnaires is to create follow-up letter that will highlight the most obvious discrepancies for each individual stakeholder involved in our survey. The aim is to stay in contact and request regular information about implementation of GDPR processes with their cloud provider. These letters will also include obligation of stakeholders to communicate with their Data Protection Officer in case of any cloud related topic issues.

**2. Lack of documentation**

- The stakeholders seem to have no knowledge that they are obliged to conclude Art.28 (3) contract.

- Some stakeholders do not have or asked for the Data Protection Impact Assessment. No stakeholders in question were able to provide us with the DPIA. We have received only one document focusing solely on data protection, however it is not clear whether it is legally binding document neither it is sure who is obliged by it. This document has general nature and is unclear in data protection clauses. In one case, even the records of the processing activities, which are required to be developed by processor, cloud provider expects to be delivered by the controller.

- Art, 28, art. 35, art. 30 GDPR

- Some stakeholders provided clear answers that they do not have such documentation. One stakeholder declared that the DPIA and risk assessment were prepared but they did not provide any evidence, moreover this stakeholder was not a party to the contract based on which the GDPR documentation should be prepared according the contract, which is publicly available and was provided to us.

- It is difficult to assume what are the differences between stakeholders regarding the availability of GDPR documentation. In general, there is lack of documents with all questioned/concerned stakeholders. They are aware of a risk assessment or DPIA but as data controllers, they do not possess any.

- We are planning to stay in contact with the relevant stakeholders and based on the facts provided in questionnaire, SA would summarize the main issues and request within the set deadline to report back to SA how the move forward with the correct GDPR implementation by using cloud services.

**3. International transfers and access by foreign public authorities**

- Only some stakeholder provided answers to questions about international transfers. Other stakeholders declared that they do not transfer personal data to third countries. Even though, from the answers provided by one of them, it is clear that there is transfer to third countries with regard to the utilisation of services mentioned. Unfortunately, we have no documentation available.

- Art. 44-46

- The stakeholders generally authorised cloud provider to transfer personal data to USA or other countries for the purpose of providing services. This general authorisation is supported by the specific appendix where additional requirements about transfers and Standard Contractual Clauses are included.

- Lack of knowledge of the stakeholders that they are using cloud service, which is transferring personal data to third countries. One of stakeholders claimed that they use cloud provider's services but in the questionnaire claimed that no personal data is transferred. Documents from one stakeholder present that Standard Contractual Clauses are signed only by cloud provider, not by data controller - stakeholder. From the documentation provided, it is not clear which version of SCC is valid (it seems that it is not the version of SCC provided in Commission implementing decision 2021/914 from 4 June 2021). In our point of view, the contractual agreement is unclear,

mainly, it is unclear what categories of data is transferred and to what locations and what are the purposes of the transfer.

- The relationships between different stakeholders are not clear, SA is not able to assess who is responsible for the relevant documentation, because the stakeholder who declared to perform transfers, referred to the general documentation where it is not the contractual party, but the documentation is concluded by another stakeholder. We interviewed this another stakeholder, who answered in his own questionnaire that no transfers are taking place. We will need to focus on the latter stakeholder and communicate about possible follow-up steps in order to achieve compliance. It seems that there are more stakeholders who are bound by these unclear clauses. SA needs to develop steps towards the stakeholders to convince them to re-negotiate the whole documentation about transfers based on the new SCC as a minimum obligation.

**4. Identification of roles - Controllership and sub-processors**

- Almost all stakeholders answered that they are data controllers and the cloud provider is processor. Only one stakeholder claimed that he is only user of cloud services.

- With regard to the possible use of sub-processors, they provided us with general clause from their contract about possibility to have other processor (sub-processor).

- Art. 5 (2), art. 24; 28 (2), 28 (4) and 28 (3) (d) GDPR

- In case of the concrete/specific stakeholder who is not aware of the role in terms of the GDPR, it is difficult to assess compliance with the GDPR requirements.

- With regard the engagement of other processor, two stakeholders claimed that the cloud provider does not have any sub-processor, other stakeholders pointed out to the contractual clause in their Art. 28 agreement. However, the text of the relevant clause about sub-processors in case this cloud provider is only general quotation of the relevant GDPR provisions. The Contract is stating possibility for specific or general authorisation without any possibility for data controller to object engagement of new sub-processor. As if there was just obligation to provide information from cloud provider about a new sub-processor. The scope of information that needs to be provided to data controller is not specified in the contract. Information about the consequences of disapproval to a new sub-processor is missing. On the other hand, in case of data protection rules of other cloud providers, from the documentation provided, it seems that there is prior general agreement for controller to involve sub-processor and information about new sub-processor is provided on the website of the processor (which might be continuously updated). However, the information about the engagement of sub-processor (and possibility to object by the controller) is vague – the documentation literally says that the provider provides some option to know that there is new update on the processor's website, but without any specification what some options mean and how they are implemented in practice. It seems that objection or written cancellation of the license when data controller disagrees with a new sub-processor, means termination of the affected service.

- Two stakeholders asked directly their cloud provider if there are some sub-processors engaged. Other two stakeholders simply presented the contractual clause. In general, it seems that stakeholders are not aware of any sub-processors. One stakeholder did not provide meaningful answer showing lack of any knowledge about circumstances of having another sub-processor with regard to data protection.

- In general, contract must be clear about timing of providing information and possibility to object and also provide criteria for appointing of new/another sub-processor. Interviewed stakeholders show lack of intention to consider these requirements.

**5. <u>Telemetric data</u>**

- Some stakeholders answered that they process telemetric data for the security purposes. In one case, it was difficult to assess the purpose. Two stakeholders replied that they do not process telemetric data and one replied that telemetric data is used for creation of access - based on the limited scope of personal data e.g. name, surname, telephone number, email address, job position, function or personal employment number, place of work and employer.

- 4 (1) in connection with 5 (a), 5 (b)

- In general, there is lack of knowledge about the issue. Controllers are not aware that telemetric data is personal data, they answered that telemetric data in general do not contain personal data. Consequently, there is transparency issue. Data subjects are not informed about the processing of their personal data using cloud services. From the point of view of SA and replies to the questionnaire, it is not possible to evaluate whether telemetric data is necessary and proportional for the purpose of the said processing. In case of one stakeholder, it is controversial whether telemetric data for access is actually used. Another stakeholder stated that telemetric data is not processed by cloud provider because these data is not listed in the contract with the cloud provider. However, the relevant contract specifies that other relevant data might be processed if relevant for the purpose of providing services based on that contract. Consequently SA cannot currently assess the scope of services and their purposes due to the missing documentation and lack of specification of services provided in the questionnaire.

- It seems that there are differences between stakeholders in terms of processing of telemetric data but this might be caused by the lack of knowledge about the scope of definition of telemetric data. With regard to some stakeholders, more emphasis needs to be given on the scope and purpose of telemetric data. In addition, the data is probably transferred to third countries. It seems that the same pre-formulated data protection agreement applies to all stakeholders without any limitation or assessment of responsible Stakeholder about the scope of telemetric data.

- More information about interpretation of the definition of personal data needs to be provided, although it seems difficult to set clear distinction when/at what level the telemetric data is personal data. In terms of contract, controllers should pay special attention to processing of personal data in terms of cloud services and at best to negotiate contract without processing of telemetric data if it is not necessary for the stakeholder purposes. SA will ask stakeholders to organise trainings about the cloud related topics targeting data protection obligations including telemetric data which should be provided by their Data Protection Officers and we will request them to report about this specific trainings to us.

## Part III – Actions by the SA

**1. <u>Have you taken action (i.e. fact-finding exercises, informal contact, prior consultation, investigation) towards any of the stakeholders concerning the use of cloud-based services *prior to* launching the coordinated action? Please describe the action you have taken and the outcome of this action (e.g. letter, recommendations to the stakeholder, general guidance,</u>**

**corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines).**

- No

2. **What action(s) are you planning to undertake based on the results of this coordinated action, if any? (E.g. letter, recommendations to the stakeholder, general guidance, corrective measures such as orders, injunctions with or without an incremental penalty, administrative fines). If possible, please indicate the timeline for these actions (also in case formal investigations are still ongoing).**

- At this stage, we are preparing letters to each stakeholder with specific issues identified from their questionnaire. It includes request to organise special trainings led by their Data Protection Officer targeting GDPR requirements in the context of processing of personal data in clouds and sending evidence about the content of such training to SA.

## Part IV – Other

1. **What is your general impression of the levels of awareness and compliance of the stakeholders you consulted concerning the use of cloud?**

- We realize that there is (very) low level of knowledge about the data protection obligations.

2. **Are there any other issues or topics that you would like to flag?**

- For those SA who faced similar situation – when each stakeholder shows lack of knowledge, what are they follow up steps? Do they consider starting with education or immediate enforcement?

3. **Are there any leading practices of the stakeholders you have contacted that you would like to share?**

- No