

2022 Coordinated Enforcement Action

Use of cloud-based services by the public sector

Adopted on 17 January 2023

EXECUTIVE SUMMARY

In October 2020, the European Data Protection Board (EDPB) decided to set up a Coordinated Enforcement Framework (CEF), with a view to streamlining enforcement and cooperation among Supervisory Authorities (SAs), consistently with the EDPB 2021-2023 Strategy.

In October 2021, the EDPB selected “the use of cloud in the public sector” for its 2022 Coordinated Enforcement Action.

Throughout 2022, 22 Supervisory Authorities across the EEA launched coordinated investigations into the use of cloud-based services by the public sector. The CEF was implemented at national level in one or several of the following ways: fact-finding exercise; questionnaire to identify if a formal investigation is warranted; commencement of a formal enforcement investigation, or follow-up of ongoing formal investigations.

Between November 2021 and January 2023, these SAs have discussed the aims and the means of their actions in the context of the CEF, and decided that a questionnaire would be sent to investigate public bodies. They drafted the questionnaire, then discussed the first results of their investigations, and the way they planned to bring public bodies to compliance through the CEF. Some elements, in particular the corrective measures they could decide at national level, are still under discussion.

The present joint-report aggregates the findings of all the Supervisory Authorities participating in the CEF. A particular attention is paid to 8 challenges identified by SAs during the CEF action. These include issues at the pre-contractual phase relating to the performance of a Data Protection Impact Assessment (and/or a risk assessment) and the role of the parties. With regard to the contracts with the CSP, the issues of lack of contract and difficulty to negotiate a tailored contract were identified, as well as the public bodies’ knowledge or control over sub-processors. Furthermore, challenges relating to international transfers and access by foreign public authorities are raised. Finally, processing of telemetry data and auditing are discussed.

Taking into account the possible sensitive nature and large amounts of data processed by public bodies, it is however essential that the fundamental right to the protection of personal data is guaranteed by all public administrations. The EDPB therefore underlines the need for public bodies to act in full compliance with the GDPR when using cloud-based products or services. In this regard, the report also provides a list of points of attention that stakeholders should take into account when concluding agreements with CSPs:

- Carry out a DPIA;
- Ensure that the roles of the involved parties are clearly and unequivocally determined;
- Ensure the CSP acts only on behalf of and according to the documented instructions of the public body and identify any possible processing by the CSP as a controller;
- Ensure that a meaningful way to object to new sub processors is possible;
- Ensure that the personal data are determined in relation to the purposes for which they are processed;
- Promote the DPO’s involvement;
- Cooperate with other public bodies in negotiating with the CSPs;
- Carry out a review to assess if processing is performed in accordance with the DPIA;
- Ensure that the procurement procedure already envisages all the necessary requirements to achieve compliance with the GDPR;

- Identify which transfers may take place in the context of routine services provision, and in case of processing of personal data for the CSPs' own business purposes (see related point) and ensure Chapter V provisions of the GDPR are met, also by identifying and adopting supplementary measures when necessary;
- Analyse if a legislation of a third country would apply to the CSP and would lead to the possibility to address access requests to data stored by the CSP in the EU;
- Examine closely and if necessary renegotiate the contract;
- Verify the conditions under which the public body is allowed for and can contribute to audits and ensure that they are in place.

The action undertaken by SAs in the CEF are still ongoing at national level, especially when formal investigations were launched. Accordingly, this document does not constitute a definitive statement of the actions carried out within the CEF as the purpose of this report is not to conclude on the measures to be adopted but to reflect on the actions undertaken by competent SAs and identify the possible points of attention. It may need to be updated in the course of 2023 to take into account the progress of the procedures which have not yet been completed to date and given the issues identified, further complementary work on general recommendations to public actors concerning the use of cloud service providers could be foreseen.

Table of contents

1	INTRODUCTION.....	5
2	STATISTICS	7
3	CHALLENGES IDENTIFIED DURING THE CEF ACTION	10
3.1	Data protection impact assessment (DPIA)	10
3.2	Role of the parties	12
3.3	Negotiating tailored contracts between public bodies and cloud service providers	14
3.4	Sub-processors	15
3.5	International transfers.....	17
3.6	Risk of access by foreign governments when using non-EU CSPs storing data in the EEA...	18
3.7	Telemetry/diagnostic information.....	19
3.8	Auditing	20
4	ACTIONS TAKEN BY SAS	21
5	POINTS OF ATTENTION FOR PUBLIC BODIES.....	30
6	CONCLUSION.....	33
	Annex 1: Definitions.....	34

1 INTRODUCTION

In October 2020, the European Data Protection Board (EDPB) decided to set up a Coordinated Enforcement Framework (CEF)¹. The CEF is a key action of the EDPB under the second pillar of its 2021-2023 Strategy², together with the creation of a Support Pool of Experts (SPE), aiming at streamlining enforcement and cooperation among supervisory authorities (SAs).

The EDPB selected in October 2021 “the use of cloud in the public sector” for its 2022 Coordinated Enforcement Action. The reasons for this prioritisation are mainly threefold:

- (i) it is essential that the fundamental right to the protection of personal data is guaranteed by all public administrations³,
- (ii) public authorities are processing large amounts of personal (and sometimes sensitive) data, and
- (iii) the rapid development of cloud technology in all sectors is creating new risks that need to be dealt with appropriately.

The uptake of cloud services⁴ has doubled for enterprises across the EU between 2016 and 2021 according to Eurostat⁵. In the public sector, the COVID-19 pandemic has intensified a digital transformation of organisations, with many public sector organisations turning to cloud services. However, in doing so, public bodies at national and EU level may face difficulties in obtaining IT products and services that comply with EU data protection rules. Because of the nature of the data processed by public administrations and the (potentially) large amount of data stored in the cloud, it is of great importance that the fundamental right to protection of personal data is properly guaranteed in all public services. All individuals (citizens as well as persons working for public services,) should be able to trust that public bodies handle their personal data with care, especially when it is processed by a third party.

Building on common preparatory work, the EDPB announced the initiation of the action on 15 February 2022. Throughout 2022, supervisory authorities across the EEA launched coordinated investigations into the use of cloud-based services by the public sector. The CEF was implemented at national level in one or several of the following ways: fact-finding exercise; questionnaire to identify if a formal investigation is warranted; commencement of a formal enforcement investigation, or follow-up of ongoing formal investigations.

Around 100 public bodies in total were addressed across the EEA, including EU institutions, covering a wide range of sectors (such as health, finance, tax, education, central buyers or providers of IT services).

¹ EDPB Document on Coordinated Enforcement Framework under Regulation 2016/679 (EDPB, 20 October 2020) <https://edpb.europa.eu/our-work-tools/our-documents/other/edpb-document-coordinated-enforcement-framework-under-regulation_en>.

² EDPB Strategy 2021-2023, adopted on 15 December 2020.

³ Letter of the Dutch Data Protection Authority to the Dutch Minister for Digitalisation on the Central Government Cloud Policy 2022, 11 November 2022, p. 1.

⁴ By “cloud services”, we mean one or more capabilities offered via cloud computing invoked using a defined interface. By “Cloud computing” we mean a paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand. (see annex 1)

⁵ Cloud computing used by 42% of enterprises (Eurostat, 09 December 2021), <https://ec.europa.eu/eurostat/web/products-eurostat-news/-/ddn-20211209-2>.

The present joint-report aggregates the findings of all the supervisory authorities participating in the CEF, and provides a state of play of their work. In particular, the first part of this report presents statistics on the stakeholders addressed, while the second part analyses the challenges faced by public bodies when procuring cloud services. In particular, SAs explored public bodies' challenges with GDPR⁶/EUDPR⁷ compliance, as appropriate⁸, when using cloud-based services. These challenges related to the process and safeguards implemented when acquiring cloud services, international transfers in view of the Schrems II judgment⁹, and provisions governing the controller-processor relationship.

For each identified challenge, we present a short description of the issue at hand, which provisions of the GDPR apply and why this has been an issue for the participating stakeholders. In addition, we present an overview of the actions already implemented, including guidance, letters, enforcement actions or potential actions by SAs or stakeholders.

With this first CEF action, the EDPB intends to:

- **foster GDPR-compliance of products and services, relying on cloud-based solutions, by the national and EU public sector;**
- **generate a deeper insight and allow targeted follow-up at EU level;**
- **promote leading practices through coordinated guidance and action, thereby ensuring the adequate protection of personal data.**

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 As regards the EDPS, any references to the GDPR should be understood as corresponding references to the EUDPR.

⁹ Facebook Ireland and Schrems (Schrems II), C-311/18, ECLI:EU:C:2020:559.

2 STATISTICS

The SAs decided to contact stakeholders from multiple categories. Eleven (11) SAs indicated that they have contacted a ministry of the central government (AT, BE, CZ, EDPS, EL, IT, SI, SK, EE, ES, FR), while 11 SAs have contacted independent public bodies of the central government (BE, CZ, EDPS, EL, FI, LT, SE, SK, EE, ES, PT)¹⁰. The EDPS, EL, LI, NL, FI and CY SAs have contacted buyers and vendor managers for the central government¹¹. The PT SA has contacted a public buyer for the public health sector.

Publicly owned companies acting as processors for several public bodies have been contacted by the DE SAs, while ministries of the regional government were part of the CEF action by the BE, DE and IT SAs. An independent public body of the regional government, a buyer for the regional government and a publicly owned company acting as a processor for several regional public bodies have been contacted by the EE, IS, and IT SAs respectively. Additionally, the BE SA has contacted a publicly owned non-profit organisation 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. Finally, the SI SA has contacted 3 public research institutes.

The SAs decided to contact stakeholders from multiple sectors. From the data gathered:

- the majority of SAs contacted stakeholders in the **digitalisation of the public administration/e-government sector** (BE, CZ, DE, EDPS, EL, FI, IT, SE, SK, CY, PT),
- the BE, DE, EDPS, EL, EE, ES, PT SAs decided to contact stakeholders that are active in the **health sector**,
- stakeholders in the **employment** sector were contacted by five SAs (CZ, DE, EDPS, EL, SE, and FR),
- the SE, SK, EDPS, EE, ES SAs contacted stakeholders in the **infrastructure sector**¹²,
- the AT, BE, EDPS, IS, SI, FR and EE SAs contacted stakeholders in the **education sector**,
- the EDPS, SE, SK, and ES SAs contacted stakeholders in the **finance sector**,
- the EDPS and the ES SA also contacted stakeholders in the **justice sector**,
- the LT SA specifically mentioned that they contacted **Statistics Lithuania**.

Additionally, the CZ SA contacted the Ministry of Interior, the DE SA contacted a stakeholder in the pension insurance sector, while the EL SA contacted a stakeholder in the immigration and asylum sector. The FR SA also investigated the Ministry of Ecological Transition, the Ministry of Culture and the Ministry for Europe and Foreign Affairs. The LI SA contacted the IT department as the buyer for the central government, the SE SA contacted three stakeholders in the social insurance sector, and the PT SA contacted a stakeholder in the social security sector. Moreover, the ES SA contacted stakeholders in the economic affairs, research, culture, and agriculture sectors and the SK SA contacted stakeholders that are active in the audit and statistics sector. Furthermore, by contacting

¹⁰ In 2022, the EDPS has formally contacted five EU institutions, bodies, offices and agencies ('EU institutions and bodies'), which are classified, in the context of this report, as equivalent to a "ministry of the central government" or "independent public body of the central government".

¹¹ The CY SA 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. The EDPS contacted a buyer for other EU institutions and bodies, equivalent to "a buyer for the central government". The EL SA indicated that the buyer is a ministry of the central government, the Ministry of Digital Governance. The Ministry of Digital Governance offers cloud services through the governmental Cloud (G-Cloud) to public bodies of every sector. The NL SA contacted 3 vendor managers for the central government.

¹² The SE SA contacted the Swedish Mapping, Cadastral and Land Registration Authority, the Swedish Civil Contingencies Agency and the Swedish Transport Administration.

processors acting for several public national and regional bodies, several sectors were involved in the actions of the IT SA such as health, finance, education.

In addition, some SAs (EDPS, DE, EL, LI, FI, and NL SAs) contacted central buyers or vendor managers that offer services to public bodies in all sectors. The SK and CY SAs indicated that the buyer they contacted offers services in the digitalisation of the public administration/e-government sector. The education sector was targeted by the buyers contacted by the IS and SI SAs, the health sector by the buyer contacted by the PT SA. The NL SA indicated it contacted vendor managers that 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 vendor managers, according to the NL SA, is to negotiate a legal/procurement framework with the CSP in order to facilitate the possible use of products and services by the organisations. Generally, the vendor managers do not buy products and services and do not commit to buy products and services as part of the legal framework, although this may happen in some cases. It is usually 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.

With regard to the number of stakeholders that the buyer provides services for, the majority of SAs responded that this information was not available to them or that the question was not applicable to them (AT, BE, CZ, DE, FI, IT, LT, NL, SE, SK, EE, ES, PT). Nevertheless, 6 SAs (EDPS, EL, IS, LI, SI, CY) specified the number of stakeholders to whom the buyer provides services. The answers provided varied, as the SI SA stated that the buyer provides services for 5 stakeholders, while the EL SA responded that the buyer provides services for approximately 150 public bodies¹³.

The majority of SAs (BE, CZ, DE, EE, EL, FI, IT, LI, LT, NL, SE, SI, SK, CY, ES) stated that the initial procedural framework of their action was fact finding that could in most cases serve to determine follow-up action based on the results. Some SAs also conducted or complemented existing formal investigations: the IT SA's action included new and ongoing investigations; new investigations have been launched by the AT, FR, PT and IS SAs, while there were ongoing investigations for the EDPS, and LT SAs.

The majority of the stakeholders (87 out of the 98 stakeholders that have been contacted) indicated that they use cloud service providers (CSPs) or are planning to do so by the end of 2022, reflecting the ever-increasing use of CSPs by public authorities. The majority of these stakeholders that use CSPs or are planning to do so in the near future (66 out of the 87) use cloud for internal organisation functions, including office suites, internal communication and human resources. Nevertheless, it is important to note that 48 stakeholders use CSPs for the exercise of public functions, such as services to citizens and processing of citizen's data.

Overall, in their investigations, SAs identified the involvement of the following most commonly used CSPs: Microsoft, Amazon, Citrix, IBM, OVH, Fujitsu, Oracle, Adobe, and Google. These CSPs provide the services themselves or the services are using the infrastructure of these companies.

In relation to the actions taken by stakeholders prior to or during the acquisition of a CSP, 32 out of the 87 stakeholders performed a data protection impact assessment (DPIA). Out of the 32 stakeholders that performed a DPIA, 21 specifically analysed transfers to third countries (sometimes called DTIA for Data Transfer Impact Assessment). 48 out of the 87 stakeholders contacted the DPO for advice while 41 stakeholders performed a general risk analysis. 11 out of the 87 stakeholders contacted the SA for advice.

¹³ According to the EL SA, the number of 150 public bodies is taken from the publicly available information published by the central buyer at <https://www.gsis.gr/ggpsdd/orama-apostoli>.

Finally, 36 out of the 87 responding stakeholders monitor technical and organisational measures to ensure compliance. With regard to international transfers, 25 out of 87 stakeholders indicated that they have adopted technical and organisational measures, and are monitoring if changes in the regulatory landscape occur (e.g., the CJEU's judgment in the Schrems II case). Finally, only 35 out of the 86 stakeholders are conducting regular risks assessments.

3 CHALLENGES IDENTIFIED DURING THE CEF ACTION

This section of the report analyses some of the challenges identified during the CEF action, both by the participating SAs and/or public bodies. These include issues at the pre-contractual phase relating to the performance of a DPIA (and/or a risk assessment) and the role of the parties. With regard to the contracts with the CSP, issues of lack of contract¹⁴ and difficulty to negotiate a bespoke contract were identified. Furthermore, challenges relating to international transfers and access by foreign public authorities, for example, transfer awareness and access by foreign governments also in the case of use of non-EU CSPs providing services only from the EEA, are raised. Finally, processing of telemetry data and auditing are discussed.

3.1 Data protection impact assessment (DPIA)

According to Article 35 (1) of the GDPR, “where processing of personal data is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall carry out a DPIA prior to processing. A single assessment may address a set of similar processing operations that present similar high risks.”

Article 35 (3) (b) of the GDPR also provides that a DPIA 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 of the GDPR.

It can be assumed that many public sector processing operations relying on cloud services would be likely to result in a high risk to the rights and freedoms of natural persons (for instance due to processing of sensitive data or data of a highly personal nature-- like health data or personal data relating to criminal convictions and offences referred to in Article 10 of the GDPR-- and processing is on a large scale). In such cases, controllers have the obligation to perform a DPIA prior to the processing. According to the EDPB Guidelines on Data Protection Impact Assessment (DPIA), “in order to provide a more concrete set of processing operations that require a DPIA due to their inherent high risk [...] nine criteria should be considered [...] In most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out¹⁵”. In addition, when a DPIA is not required, the appropriate technical and organisation measures should nevertheless be determined following a risk assessment, pursuant to Article 32 of the GDPR.

However, **only thirty-two out of the eighty-six stakeholders that use CSPs indicated that a DPIA has been conducted**, before the intended processing itself. The EDPB would like to reiterate that the deployment of cloud services by public bodies will often trigger a likely high risk under the GDPR. Based on the information received by SAs from public bodies, in many cases where no DPIA was not carried out, the reason for not doing so was unclear for SAs¹⁶. This could be a potential violation of the GDPR. Public bodies that have not (yet) conducted a DPIA when deploying cloud services should therefore (re)evaluate in the short term whether a DPIA should be conducted and document this evaluation.

In some cases, **stakeholders confirmed that a DPIA was performed but it was not clear whether it took any specificity of cloud services into account**.

¹⁴ In the sense of Article 28 GDPR.

¹⁵ 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.9 and 11.

¹⁶ The reasons provided for not carrying out a DPIA included that the processing is carried out in the context of the use of cloud services, which do not, according to stakeholders, meet the conditions, listed either in Article 35 (3) of the GDPR or in the list established by each Supervisory Authority under Article 35(4) of the GDPR.

Some stakeholders have also relied completely on the security measures by the CSP, or may have considered that a DPIA was neither necessary nor mandatory. It is important to note that where cloud service providers have provided a risk assessment to the controller, this was usually an information security risk assessment. Data protection risks have generally not been sufficiently assessed in this exercise as the service provider is not aware of (i) what and how specific processing activities are taking place, (ii) the purposes of the processing and, consequently, (iii) the risks that this processing imposes on the rights and freedoms of natural persons (rather than the risks on the public body itself).

In addition, although Article 35 (1) of the GDPR provides that, when a DPIA is required, it must be carried out prior to the processing, a number of stakeholders carried out an initial DPIA only after the processing commenced.

According to Article 35 (2) of the GDPR: **“the controller shall seek the advice of the data protection officer**, where designated, when carrying out a data protection impact assessment.” However, the data protection officer (DPO) of the controller, in most cases, was not closely involved in the process. This raises concerns amongst some SAs. Close involvement of the DPO can in fact aid public bodies to implement cloud applications in a way that is compliant with the GDPR.

As stated in the Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of the GDPR, “this advice, and the decisions taken by the controller, should be documented within the DPIA.”¹⁷ The DPO should also monitor the performance of the DPIA, pursuant to Article 39(1)(c) of the GDPR. Further guidance is provided in the WP29 Guidelines on Data Protection Officer 16/EN WP 243. In addition: “it is good practice to define and document other specific roles and responsibilities, depending on internal policy, processes and rules, e.g.: [...] the Chief Information Security Officer (CISO), if appointed, as well as the DPO, could suggest that the controller carries out a DPIA on a specific processing operation, and should help the stakeholders on the methodology, help to evaluate the quality of the risk assessment and whether the residual risk is acceptable, and to develop knowledge specific to the data controller context”.

According to Article 35 (11) of the GDPR, where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the DPIA at least when there is a change of the risk represented by processing operations. In this respect, **a switch to cloud services may be a change of the risk that would need to entail a review of the DPIA, and a periodic review may be needed.**

The lack of a DPIA, where necessary, may result in 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 also face difficulties fulfilling their accountability obligation to use only processors providing sufficient guarantees, according to Article 28 (1) of the GDPR (see also section 3.3).

¹⁷ EDPB 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. 15.

3.2 Role of the parties

According to Article 4 (7) of the GDPR, the ‘controller’, alone or jointly with others, determines the purposes and means of the processing of personal data. “The concept of controller and its interaction with the concept of processor play a crucial role in the application of the GDPR, since they determine who shall be responsible for compliance with different data protection rules, and how data subjects can exercise their rights in practice.

Furthermore, pursuant to the accountability principle, the controller shall be responsible for, and be able to demonstrate compliance with, the principles relating to processing of personal data in Article 5 of the GDPR¹⁸.” The accountability principle is further elaborated in Article 24 of the GDPR, which states that the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR. Such measures shall be reviewed and updated if necessary. The accountability principle is also reflected in Article 28 of the GDPR, which lays down the controller’s obligations when engaging a processor.”¹⁹

In order to fully assess the roles of the parties when using a CSP, it is important that all (subsequent) processing activities are determined. A role under the GDPR is always linked to a set of processing activities and a CSP might also, for instance, process personal data, according to Article 6 (1) (b) of the GDPR, necessary for providing the services requested by a public body. In its Guidelines on the concepts of controller and processor in the GDPR, the EDPB reminded that the Article 29 Working Party had previously stated that “the concepts of controller and processor are functional concepts: they aim to allocate responsibilities according to the actual roles of the parties. This implies that the legal status of an actor as either a “controller” or a “processor” must in principle be determined by its actual activities in a specific situation, rather than upon the formal designation of an actor as being either a “controller” or “processor” (e.g. in a contract) ”²⁰. Therefore, another key issue when procuring CSPs is the contractual allocation of the roles of controller and processor, and in particular, whether it corresponds to the factual circumstances. In most cases, the public bodies act and present themselves as controllers and the CSPs (including hyper-scalers) as processors or sub-processors. However, if there is imbalance of power between a hyper-scale CSPs and a public body, it can be difficult for the public body as a controller to negotiate the terms of the contracts in practice²¹.

If the roles and responsibilities are not correctly specified, the compliance with the respective obligations of the CSP and of the public bodies under the GDPR becomes difficult. This is because it is not clear to which extent the CSP should for example, help the public bodies to perform a DPIA, or in case data subjects exercise their rights regarding data processing in the cloud, respond to them appropriately on behalf of the public bodies. The underlying objective of attributing the role of controller is to ensure accountability and the effective and comprehensive protection of the personal data²². Clear definition of the processing activities and respective tasks allocated to CSPs are key to

¹⁸ EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, adopted on 7 July 2021, p. 7.

¹⁹ EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, adopted on 7 July 2021, p. 8.

²⁰ EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, adopted on 7 July 2021, p. 9; See also CJEU Case C-40/17 Fashion ID.

²¹ Nevertheless, at first glance, in such situation, and as illustrated in the Guidelines on the concept of controller and processor in the GDPR, the public bodies should still be considered as a controller, given its decision to make use of a particular CSP in order to process personal data for its purposes.

²² EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, adopted on 7 July 2021, p. 9.

allow the public bodies to identify and fulfil all their responsibilities arising from the GDPR for the processing for which they are controllers, including their accountability obligations, as per Article 5 (2) of the GDPR.

Furthermore, “the accountability principle together with the other, more specific rules on how to comply with the GDPR and the distribution of responsibility therefore makes it necessary to define the different roles of several actors involved in a personal data processing activity.”²³ In some cases, SAs noted that the CSP may contractually envisage data processing activities for which it acts as a controller, i.e. it processes data relating to the activities of the public body for its own purposes. In particular, the role of the hyper-scalers is not always clear, especially regarding the processing of telemetry/diagnostic data that takes place for the CSPs purposes. As a result, CSPs would become independent controllers²⁴, if they alone decide the means and purposes of this processing. When the CSP is in fact a controller for some processing operations, the onus is on them to inform data subjects, and comply with other obligations of the GDPR, e.g., accountability obligations as per Article 5 (2) of the GDPR. In addition, a legal basis for handing over of personal data by the public body and for the processing activities carried out afterwards by the CSP acting as a controller is needed. If the public body does not have such a legal basis for disclosing the personal data to the CSP, it cannot comply with the provisions of the GDPR. This can lead to situations in which a public body enables the processing of personal data from civilians and employees entrusted to the public body, by a commercial enterprise for its own purposes in violation of GDPR.

With regard to central buyers, public bodies have sometimes indicated that they considered that the central buyer has a role of processor and even in some cases, a role as an independent or joint data controller, because the central buyer has the ability to decide on the means of the processing and the selection of processors/sub-processors for providing the cloud services²⁵. Yet, notwithstanding the complexity of the model and the difficulty to clarify the respective roles of each parties, including of the central buyers, this should not lead SAs to consider central buyers as processors or joint controllers as it is not clear, in these situations, what processing the central buyers would actually carry out.

As mentioned before, a public body processing personal data and choosing a CSP is a controller and responsible for engaging with a CSP in a GDPR-compliant way. However it is important to note that “both controllers and processors can be fined in case of non-compliance with the obligations of the GDPR that are relevant to them and both are directly accountable towards SAs by virtue of the obligations to maintain and provide appropriate documentation upon request, co-operate in case of an investigation and abide by administrative orders.”²⁶

²³ EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, adopted on 7 July 2021, p. 8.

²⁴ in such a situation, CSPs and public bodies could also qualify as joint controllers together with the public bodies if they jointly determine the purposes and means of processing. In order to be permissible, this requires that an adequate legal basis and an agreement pursuant to Article 26 of the GDPR exists. This option should not be considered when the legal basis for processing by the public body is the necessity for the performance of a task carried out in the public interest by a public body.

²⁵ see p4

https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/brief_over_inzet_cloud_service_providers.pdf

²⁶ EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, adopted on 7 July 2021, p. 8.

3.3 Negotiating tailored contracts between public bodies and cloud service providers

According to Article 28 (1) of the GDPR: “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 the GDPR and ensure the protection of the rights of the data subject.”

According to Article 28 (3) of the GDPR: “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.” Article 28(3) of the GDPR lists elements that need, in particular, to be included in the contract. In practice, this means that when a public body decides to use a CSP, a bespoke contract may need to be negotiated and the terms of each processor agreement need to be tailored to the processing operation(-s), even if a standard contract is used as a template²⁷.

In addition, according to Article 28 (10) of the GDPR: “without prejudice to Articles 82, 83 and 84, if a processor infringes the GDPR by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.”

A contract or other legal act pursuant to Article 28 (3) of the GDPR has not been established between some of the public bodies and the respective CSP, even though the processing is already ongoing. In the majority of the investigated cases, it was claimed to be difficult for the participating stakeholders to negotiate a bespoke contract, considering that CSPs generally offer standard, predetermined contracts and left no room for negotiating the terms of the contracts. The public bodies, in these cases, are often the parties with less bargaining power. Due to the imbalance of power between the parties, the participating stakeholders found themselves in situations where they could either accept the terms and conditions offered in pre-specified contracts by the CSP or decide not to use the cloud service, as there was little or no possibility to negotiate additions or amendments to it. There are however situations in which public bodies or buyers were able to negotiate bespoke contracts²⁸. In general, public bodies in the EEA could and should, before claiming an imbalance of power, do more in using existing and often freely available information from these cases²⁹ and join forces to counter the imbalance of power.

If the public bodies cannot negotiate the terms of the contracts in practice, due to the imbalance of power, it may be difficult for them to determine the purposes and the means of the processing of personal data for the duration of the contract, and fulfil their obligations under the GDPR³⁰. In this

²⁷ If a standard contract is used, the specifics of the processing on behalf of the public body will always need to be included in the contract or its annexes

²⁸ The standard contractual clauses on controller / processor can also be helpful as a guidance when drafting bespoke contracts in this type of relation. The EDPB has already issued opinions on the EU Commission SCC but also on SCC adopted by DK SA, SI SA, and LT SA. See [Opinions | European Data Protection Board \(europa.eu\)](#)

²⁹ See for instance <https://slmmicrosoftrijk.nl/downloads-dpias/>

³⁰ As stated in the Guidelines on the concepts of controller and processor in the GDPR, “the fact that the contract and its detailed terms of business are prepared by the service provider rather than by the controller is not in itself problematic and is not in itself a sufficient basis to conclude that the service provider should be considered as a controller. In addition, the imbalance in the contractual power of a small data controller with respect to big service providers should not be considered as a justification for the controller to accept clauses and terms of contracts, which are not in compliance with data protection law, nor can it discharge the controller from its data protection obligations. The controller must evaluate the terms and in so far as it freely accepts them and makes use of the service, it has also accepted full responsibility for compliance with the GDPR”. Therefore, and as illustrated in two examples provided in these Guidelines, the public body should still

situation, where some of the purposes and means are defined by the CSP, the service provider would then be considered as an autonomous controller, according to Article 28 (10) of the GDPR and will be liable for the violation of the relevant provisions of the GDPR (e.g., lack of appropriate legal basis, information to be provided to data subjects for such processing activities, etc.). In such cases, also the public body handing over personal data to the CSP and losing control over those personal data would infringe the relevant GDPR provisions (e.g. lack of appropriate legal basis needed for providing personal data by the public body to the CSP, the information to be provided to data subjects in relation to this processing operation, etc.).

In some of the cases with a central buyer, the contract with the reseller referred explicitly to specific future agreements/contracts to fulfil the requirements of Article 28 (3) of the GDPR; however, such contracts were not presented to the SAs that conducted the CEF action.

3.4 Sub-processors

Article 28(1) of the GDPR provides that controllers must “*use only processors providing sufficient guarantees*” so that the processing meets the requirements of the GDPR.

According to 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.

According to Article 28 (4) of the GDPR: “where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation.” Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

Based on the CEF action, it appears that, in many cases, the public bodies’ knowledge or control over sub-processors involved in the processing and the extent of such processing is mainly limited to general information made available by the hyper-scalers.

In particular, most public bodies seem to have limited control over and cannot object meaningfully to the use of sub-processors or to changes of sub-processors without risking a potentially critical loss of service. When asked about sub-processors by SAs, many respondents either did not provide any information or they referred to an online list with the sub-processors of the CSPs³¹. In those cases, this

be considered as a controller, given its decision to make use of a particular cloud service provider in order to process personal data for its purposes. Insofar as the CSP does not process the personal data for its own purposes (with an appropriate legal basis under Article 6) and stores the data solely on behalf of its customers, the service provider shall be considered as a processor.

³¹ See below, for example the lists provided by various hyperscalers.

Microsoft: <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.

is an indication that the public bodies' knowledge on sub-processors may be limited to the publicly available information by the CSP, and that public bodies do not have control over the use of sub-processors, such as knowing exactly which one is involved for what specific purposes in their particular usage of the cloud or having the chance to approve or object to a specific sub-processor.

The fact that public bodies have actually no control over the engagement of processors 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. However, it must be emphasised that this difficulty does not, in itself, exonerate the controller from its responsibilities in the processing.

Moreover, the question of whether the controller is offered a meaningful opportunity to object to changes of sub-processors was also addressed. In some cases, the public bodies had provided a general authorisation to contract sub-processors, but the controllers had no meaningful right to object, no efficient objection procedure existed (timeline, consequences etc.) and no exit strategy had been included in the processor contract³². In practice, in the cases investigated in the CEF action, several CSPs inform their customers about changes made to the sub-processors in their newsletter or on their website, but the possibility for controllers to object to the use of such processor is often limited to termination of the contract. Pursuant to Article 28 (2) of the GDPR, controllers must be offered a way to either authorise or object (in case of a general written authorisation) to the addition or replacement of other processors. The risk of not having a meaningful way to object should be assessed prior to choosing a CSP.

In addition, the contract or other legal act shall stipulate, according to Article 28 (3) of the GDPR, that the processor respects the conditions referred to in paragraphs 2 and 4 of Article 28 of the GDPR for engaging another processor. Therefore, when there is a lack of contract between the public authority and the CSP, it is a strong indication that the framework for engaging other processors is not clearly determined.

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

In this regard, differences have been identified between some of the CSPs whose services were subject to the CEF action. In one of the CSPs contracts, for example, the terms merely repeat the text of Article 28 (2) of the GDPR. Another CSPs standard contracts describes a timeline (notification period) and foresees that in case of an objection the public body and CSP will try to find a solution addressing such objection (e.g. including making the services available without the involvement of the relevant third-party sub-processor). In general, the risk of not having a meaningful way to object to a new sub-processor seems often to be underestimated, ignored or hoped to be handled when the issue arises. This can lead to a problem of a CSP using an unwanted subprocessor and a public body not being able to change CSP, and thus to non-compliance with GDPR.

Google: <https://workspace.google.com/terms/subprocessors.html>;

AWS: <https://aws.amazon.com/compliance/sub-processors/>

Oracle maintains lists of Oracle Affiliates and Third Party Sub-processors that may Process Personal Information available to controllers in their Support Section.

³² There are rarely tools, procedures, standard data formats or services interfaces that could guarantee data, application and service portability (reversibility).

3.5 International transfers

In the context of the provision of cloud services, transfers may generally be envisaged in the context of routine services provision (e.g. in the cases of ‘round the clock’ services), in case of processing of personal data for the CSPs’ own business purposes (see related point) and in case of request of access to personal data by third country public authorities (see later in the text).

During the CEF action, several SAs reached out to public bodies in the EEA using hyper-scale cloud-based services, in particular software as a service (SaaS), provided by non EU-based (including US based companies). Some of these companies are based or are operating in third countries that do not offer a level of protection that was recognised as adequate according to Article 45 of the GDPR. Therefore, a public authority’s use of the software provided by the CSP, may involve transfers to many destinations that fail to ensure an essentially equivalent level of protection to the EU, including the United States of America (US). In such cases, the public body – acting as the controller – should carefully assess the transfers that may be carried out on its behalf by the CSP, e.g. by identifying the categories of personal data transferred, the purposes, the entities to which data may be transferred and the third country involved. The assessment of the international transfers of personal data taking place should be done prior to engaging with the CSP. Public bodies should provide instructions to the processor in order to identify and use a proper transfer tool and, if necessary, to identify and implement appropriate supplementary measures which ensure that the safeguards contained in the chosen transfer tool may be complied with by the importer so as to ensure that the level of protection afforded by the GDPR is not undermined when data are transferred to a third country.

When information available to the public bodies as a controller and to the supervisory authority is not sufficiently clear, it can be difficult to assess precisely what categories of data are transferred to what locations and for what purposes.

In addition, especially in the context of some SaaS implementations, it can prove impossible or extremely challenging to identify effective supplementary measures. Therefore, it would be extremely likely that the transfers would take place in breach of the transfer rules (*Schrems II* ruling), requiring the public bodies acting as controllers to identify different solutions in order to prevent or stop such transfers³³ e.g., by (re)negotiating contracts or using different cloud solutions which are compliant with the GDPR (e.g. compliant EEA-sovereign cloud solutions).

Finally, the results of the co-ordinated action show that in many cases, the choice of CSP was de facto made by a central buyer for the public administrations. It is therefore important to ensure that services are assessed by the central buyers in the first place so as to identify and propose to public bodies only those services which are compliant with GDPR, as this will foster compliance by design of all the public bodies using these solutions, also considering that each public body alone may not have the same negotiation power vis-à-vis the CSPs than when joining forces.

³³ See for further information on international transfers in the context of the *Schrems II* decision: Recommendation 1/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

3.6 Risk of access by foreign governments when using non-EU CSPs storing data in the EEA

The analysis of the documents received by the authorities participating in the CEF action shows that the issue of access by third country public authorities to data stored or processed within the EEA has indeed been identified by several controllers but is usually not sufficiently tackled by them, both legally and technically.

Several provisions of the GDPR require the controller/processor to ensure the protection and confidentiality of data it processes:

Firstly, **Article 28** GDPR provides for the specific obligations when processors are involved.

Indeed, Article 28(1) of the GDPR provides that 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 the GDPR and ensure the protection of the rights of the data subject. Processing carried out by a processor shall also be governed by a binding contract ensuring the respect of a number of obligations such as security and confidentiality obligations taking into account among others the nature and purpose of the processing, the type of personal data, the specific tasks and responsibilities of the processor, as well as the risk to the rights and freedoms of the data subject (see Recital 81 GDPR).

Whereas Article 28(3) (a) of the GDPR provides for a possibility for processors to lawfully disregard the controllers' instructions in order to comply with legal obligations under EU/EEA laws, *e contrario* this possibility does not extend to compliance with third country legal obligations.

Indeed, such access requests by third country authorities appear to be envisaged by multiple CSPs who are part of multinational groups whereas their data processing agreements pursuant to Article 28(3) explicitly include clauses such as

"If [CSP] receives a legally binding request for disclosure of personal information which is subject to this Policy, [CSP] will notify the controller promptly unless prohibited from doing so by a law enforcement authority and put the request on hold and notify the lead data protection authority and the appropriate data protection authority competent for the controller unless legally prohibited from doing so or where there is an imminent risk of serious harm. If [CSP] is legally prohibited from putting the request on hold, it will inform the requesting authority about its obligations under European data protection law and ask the authority to waive this prohibition. Where such prohibition cannot be waived, [CSP] will provide the competent data protection authorities with an annual report providing general information about any such requests for disclosure it may have received, to the extent legally permitted to do so"

or

"[CSP] will not transfer Customer Data from Customer's selected Region(s) except as necessary to provide the Services initiated by Customer, or as necessary to comply with the law or binding order of a governmental body."

Secondly, from a legal point of view, **Article 48** provides that "any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on

an international agreement [...] in force between the requesting third country and the EU or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter”³⁴.

Additionally, **Articles 5(1)(f), 24**, and, from a technical point of view, **Article 32 of the GDPR**, require the controller/processor to implement appropriate technical and organisational measures to ensure, in particular, the confidentiality of processing systems and services in order to mitigate the risk of unauthorised and unlawful disclosure of or access to personal data processed.

It stems from the analysis made by the authorities that the sole use of a CSP that is part of a multinational group subject to third country laws may result in the concerned third country laws also applying to data stored in the EEA. Possible requests would in this case be addressed directly to the CSP within the EEA and would concern data present in the EEA and not data already undergoing transfer. In this context, the controller/CSP would therefore not necessarily have made the assessment of this legal framework with a view to apply the relevant safeguards. The analysis of all the elements that may lead to different situations and different violations of the aforementioned relevant provisions of the GDPR in respect of the processing carried out by the processor (acting as an autonomous controller under Article 28(10) of the GDPR when it acts in violation of the instructions of the controller) and/or by the public authority itself if appropriate instructions are not provided according to Article 28(3) of the GDPR or a processor not providing appropriate safeguards as required by Article 28(1) of the GDPR is engaged.

Where the application of the legislation of the third country would lead to the possibility to address access requests to data stored by the CSP in the EEA, **a thorough analysis should therefore be made before the conclusion of the contract.**

3.7 Telemetry/diagnostic information

In order to provide the cloud services, CSPs process telemetry data, i.e. data relating to the use of infrastructures and services, for example, resource identifiers, tags, security and access roles, rules, usage policies, permissions, usage statistics by different kinds of users. In particular, telemetry data may for instance be used 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. Rules are usually set forth in order to minimize human access to usage and diagnostic data and avoid the identification of individuals. Since personal data means any information relating to an identified or identifiable natural person, it is likely that many telemetry data would qualify as personal data³⁵. From a data protection point of view, the exact role of the CSPs when processing telemetry data should be clarified. In some cases, CSPs declare that they act as controllers for the processing of telemetry data, while in other cases they consider themselves as processors on behalf of the public authorities.

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 the principles of Article 5 GDPR with particular regard to transparency, purpose limitation and data minimisation.

³⁴ National decisions have already been taken in some Member States. For instance, in its order of 13 October 2020, the French Council of State acknowledged the existence of a possibility of data transfer from the HDH following an access request (an information system designed to gather health data whose hosting has been entrusted to Microsoft) to the United States and requested additional safeguards, by extension to what is foreseen for transfers to protect personal data exposed to such access request when transferred to a third country.

³⁵ In addition, it must be highlighted that telemetry data may provide detailed information on users, for instance by gaining insight about the working times of employees.

In most cases, despite the fact that data protection risks with telemetry data were already public knowledge³⁶, **precise information was sought from the CSPs with regard to the processing of telemetry data only because of the CEF investigation activities**. Therefore, many stakeholders seemed to lack precise knowledge about the processing of diagnostic/telemetry data by CSPs and **there** were no evaluations carried out before the start of usage, and the contract did not provide clearly and precisely what data could be collected. In this respect, compliance with Article 28 GDPR needs a careful assessment if adequate data protection clauses covering also telemetry data are not included in the contract with a CSP.

Finally, only a few of the stakeholders were aware that, in the context of the processing of cloud telemetry data, data transfers to third countries took place, and that, as a result, compliance with Chapter V of the GDPR should also be ensured.

3.8 Auditing

Article 28 (3) (h) of the GDPR provides that the processor shall make available to the controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

In this respect, most stakeholders carry out periodic checks (not necessarily qualifying as audits) on the CSPs' activities through the annual verification of certification reports and the documentation made available by the CSP on their website. However, it appears that public authorities generally do not carry out specific and direct audit activities, including inspections, regarding any CSPs.

Some stakeholders indicated that generally, CSPs do not allow the performance of audits and that it is difficult to negotiate specific clauses in this regard, including 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 public authority. This may lead to situations of non-compliance with Article 28(3)(h) GDPR.

³⁶ see <https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/techblog-telemetrie-windows-10>

4 ACTIONS TAKEN BY SAS

This section presents a list of decisions or other types of actions already taken at national level in the field of cloud computing by several SAs, in reverse chronological order. In particular, this section does not aim at presenting a comprehensive overview of all actions conducted by national SAs, neither does it list ongoing actions that are not finalised and on which have not yet communicated.

The FI SA has investigated the use of learning tools provided by Google as well as cookies and other trackers by ministries and other public authorities. The FI SA is also looking into the use of cloud service providers by the city of Helsinki and the use of cookies and other trackers on the websites of online pharmacies. These investigations have not yet been finalised. . In October 2022, in the context of a prior consultation, the FI SA issued a warning to the Legal Register Centre concerning e.g., risks related to transfers of personal data to third countries. In December 2022, the FI SA issued a decision regarding the use of Google Analytics web analytics service in the Helsinki metropolitan area online library, which led to information on searched books and other items ending up at Google. The practice in place also involved unlawful data transfers to the US, and in addition to Google Analytics, the controllers used Google Tag Manager on their website (in breach of Articles 44 and 46 of the GDPR). The controllers did not have a lawful basis for processing (the cookie banner did not work), and the controllers were also considered to have breached Articles 25 and 32 of the GDPR. In addition, the controllers did not provide sufficient information on the data transfers (breach of Article 13 of the GDPR). In this decision, the Deputy Data Protection Ombudsman commented on cookies and other trackers placed on websites of public authorities, and e.g. stated that people should be able to use online services of public authorities without data collection that benefits third parties. The Deputy Data Protection Ombudsman also made a point that public authorities should not use citizens' personal data as a means of payment, and a public authority should effectively assess whether a free service (such as a web analytics service) is in fact paid for with personal data. A reprimand and an order to erase the collected data (including data transferred to the US) were issued to the controllers. It should be noted that an administrative fine cannot be issued to public authorities in Finland.

On 25 November 2022, the German Data Protection Conference ('DSK') published their evaluation of Microsoft 365³⁷. A response by Microsoft was also published³⁸. This work follows talks with Microsoft which were initiated at the Conference meeting of 22 September 2020, where a working group led by Brandenburg and the Bavarian State Office for Data Protection Supervision (BayLDA) were requested to enter into discussions with Microsoft "to achieve timely data protection corrections and adaptations to the standards of third-country transfers for the application practice of public and non-public bodies identified by the Schrems II decision of the ECJ." In particular, the evaluation indicates that in September 2022, Microsoft updated their Data Protection Addendum ('DPA'), clarifying Microsoft's responsibility for some processing operations. However, the Conference highlights that the changes do not conclusively clarify when Microsoft acts as a processor and as a controller. Additional shortcomings were identified by the Conference.

In November 2022, the French ministry of Education answered a question from a Member of Parliament. The MP alerted the government to Microsoft's free offer of Office 365 to teachers, and in particular, to the storage of personal data on a US cloud and the extraterritoriality of US law. In his answer, the minister said that the Ministry had asked the principals to stop any deployment or extension of Office 365 as well as Google solutions, which would be contrary to the GDPR. This request

³⁷ https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf

³⁸ https://news.microsoft.com/wp-content/uploads/prod/sites/40/2022/11/DSK-Blog-Post_25NOV2022_ENG_FINAL.pdf

was made in application of the circular “cloud au centre”, which invited the various ministers to ensure that the commercial cloud offers used by the public services and organisations under their authority were immune to any extra-EU regulation. The government already stated that the Microsoft 365 collaboration suite did not comply with the “cloud au centre” doctrine³⁹.

In November 2022, following the publication of a new government-wide cloud policy in the Netherlands, the NL SA sent out two advisory letters. The SA determined in the first letter that, among others, there was insufficient mentioning of data protection risks in the cloud policy.⁴⁰ The second letter was aimed at all Dutch ministries and interlinked with the first letter. In this letter, the NL SA informed all ministries of their role following GDPR when choosing to use a CSP and the importance of the role of vendor managers.⁴¹

In October 2022, the EDPS issued a decision pursuant to Article 58(3) (e) EUDPR (equivalent to Article 58(3) (h) of the 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 the use of contractual clauses until 31 October 2024 given the, inter alia, 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 followed a previous EDPS decision of August 2021⁴² authorising the use of the contractual clauses in question for 13 months.

Throughout the fall of 2022, the DK SA handled a set of related cases concerning Danish municipalities’ use of Google Workspace for Education. Originally, in September 2021, the DK SA ordered a Danish municipality to perform a data protection impact assessment in relation to their processing of personal data of the municipality’s school children by using Google Workspace for Education and Chromebooks. Upon reviewing the municipality’s documentation and assessment of the risks to the rights and freedoms of the data subjects, the SA found in July 2022 that the performed DPIA did not sufficiently address all the relevant risks of the processing activity. Consequently, the Danish DPA reprimanded the municipality for infringing a number of provisions of the GDPR, issued a ban on the use of Google Workspace for Education by the municipality, and ordered a suspension of transfer of personal data by way of Google Workspace to third countries which do not provide an essentially equivalent level of data protection. In the beginning of August 2022, the DK SA reviewed the municipalities’ renewed documentation and DPIA. Following this review, the DK SA upheld its ban on the use of Google Workspace as the assessment still did not sufficiently address the risks to the data subjects. In continuation of its decision in August, the DK SA engaged with the municipality to address and mitigate the outstanding risks, and in September 2022 the SA suspended the ban on the use of Google Workspace by the municipality conditioned on the municipality’s continued work to address and mitigate the outstanding risks together with the service provider. Under the auspices of Local Government Denmark – an organisation representing the Danish municipalities – the affected municipality along with approximately 50 municipalities which use Google Workspace in their school,

³⁹ cf. <https://www.legifrance.gouv.fr/download/pdf/circ?id=45205> and « Note aux secrétaires généraux des ministères; objet: doctrine “cloud au centre” et offre 365 de Microsoft » ; 15/09/2021

⁴⁰ <https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/ap-kabinet-moet-privacyrisico%E2%80%99s-cloudbeleid-aanpakken>

⁴¹ https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/brief_over_inzet_cloud_service_providers.pdf

⁴² 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 available at https://edps.europa.eu/system/files/2021-11/17-11-2021-edps_decision_authorising_temorarily_use_of_cjeu-cisco_ad_hoc_clauses_for_transfers_cisco_webex_1.pdf

joined together and with the service provider to address the risks identified by the DK SA. In late November 2022, the municipalities submitted their renewed documentation following their joint effort to document their mitigation of all relevant risks and their compliant use of Google Workspace, and will submit further documentation in January 2023, for the DK SA's review.

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.

The EDPS (as a supervisory authority) and other EU institutions and bodies (as controllers) have been closely involved in certain inter-institutional procurement procedures⁴³ relating to cloud services. This has allowed the relevant data protection (including 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 the 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 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 SaaS 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, the EDPS 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.

In April 2022, the EDPS published a factsheet⁴⁴ in order to share an informal supervisory opinion issued to an EU institution that requested guidance. In the factsheet, 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 as well as the EDPS' 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 concerning the transfers to countries outside the EEA and informed them of the 2022 Coordinated Enforcement Action.

In April 2022, the EDPS also issued a decision⁴⁵ to the EU agency Frontex on the latter's 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

⁴³ Both before and after the Schrems II judgment.

⁴⁴ https://edps.europa.eu/system/files/2022-04/22-04-29_ongoing-investigation-into-the-use-of-m365-by-euis_en.pdf.

⁴⁵ [EDPS Decision concerning the investigation into Frontex's move to the Cloud](https://edps.europa.eu/system/files/2022-04/2022-04-12-edps-decision-frontex_en.pdf), available at https://edps.europa.eu/system/files/2022-04/2022-04-12-edps-decision-frontex_en.pdf

EUDPR, taking the EDPS Guidelines on the use of cloud computing services⁴⁶ issued in 2018 into account. 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 of the EUDPR⁴⁷ 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.

On 20 December 2021⁴⁸ and 3 May 2022⁴⁹, the IS SA ordered the municipality of Reykjavík, to stop all processing of personal data of elementary-students in the Seesaw educational system⁵⁰, due to several infringements of the GDPR. The processing agreement was insufficient, a specified, explicit and legitimate purpose for the processing in question was not demonstrated, and the processing was neither fair nor transparent. In addition, the principles of data minimisation and storage limitation were not implemented or data protection by design and by default, considering the amount of data collected, the extent of processing, and the period of storage. The DPIA did not meet the minimum requirements, appropriate security of the data was not demonstrated, and the data was being transferred to the US without appropriate safeguards. Finally, the infringements concerned personal data of children and it was considered likely that sensitive data were being processed.

On 23 November 2021⁵¹, 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 IT SA requested clarifications in the decree about the role carried out by the Ministry and other parties involved (e.g. CSPs) 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 2021⁵², 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 also prohibited the transfer of data subjects’ personal data to the US 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).

⁴⁶ EDPS Guidelines on the use of cloud computing services by the European institutions and bodies, available at: https://edps.europa.eu/data-protection/our-work/publications/guidelines/guidelines-use-cloud-computing-services-european_en.

⁴⁷ Corresponding to Articles 5 (2), 24 and 25 of the GDPR.

⁴⁸ <https://www.personuvernd.is/urlausnir/akvordun-um-notkun-seesaw-nemendakerfisins-i-grunnskolum-reykjavikur>.

⁴⁹ In addition, the IS SA decided to impose an administrative fine.

<https://www.personuvernd.is/urlausnir/notkun-seesaw-nemendakerfisins-i-grunnskolum-reykjavikur-sektarakvordun-1>.

⁵⁰ <https://web.seesaw.me/>

⁵¹ <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9721434>

⁵² <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9703988>. The decision is currently under judicial proceeding.

On July 23, 2021, the FR SA sent a letter to the Ministry of Health asking it to take the necessary measures to ensure the compliance of the "TOUSANTICOVID" application (which allowed users to store their Covid certificate). Indeed, during audits conducted by the FR SA, the CNIL noted that the content of the barcode was transmitted via servers located partly in the United States in order to secure the information systems used (distributed anti-denial of service device and firewall). In its letter, the FR SA asked the Ministry to consider a change of service provider in order to use a solution from a company subject to the exclusive jurisdiction of the European Union. In the meantime, the FR SA also requested that certificates to be converted be end-to-end encrypted. As of August 2, 2021, the end-to-end encryption of certificates during their transmission was effectively implemented, thus allowing the compliance of the processing. No unencrypted data relating to the evidence constituting the Covid certificate has since been transmitted to servers located outside the European Union.

In July 2021, the EDPS issued an opinion⁵³ in response to a request for prior consultation under Article 40 EUDPR⁵⁴ 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 the 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 requirements of the EUDPR 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 EUDPR⁵⁵. Moreover, the EDPS made several recommendations to assist the institution in ensuring compliant processing.

In July 2021, the EDPS issued another opinion⁵⁶ in relation to transfers to a third country. The opinion included guidance on the use of derogations under Article 50 EUDPR⁵⁷ for transfers carried by a CSP for the purposes of publishing a newsletter by an EU agency. In particular, the EDPS 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 US.

In June 2021⁵⁸, as a result of an 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 tax payments, digital Covid certificates, 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

⁵³ [EDPS Opinion on a prior consultation requested by the European Central Bank on their new customer relationship management system](https://edps.europa.eu/system/files/2022-04/21-07-08_edps_opinion_ecb_customer-management-system_en.pdf), available at https://edps.europa.eu/system/files/2022-04/21-07-08_edps_opinion_ecb_customer-management-system_en.pdf

⁵⁴ Corresponding to Article 36 of the GDPR,

⁵⁵ Corresponding to Articles 5(2), 25, 28, 44 and 46 GDPR

⁵⁶ [EDPS Opinion on transfers to a third country resulting from the use of a newsletter service by ENISA](https://edps.europa.eu/system/files/2021-09/21-07-27_opinion_enisa_transfers_third_countries_en.pdf), available at https://edps.europa.eu/system/files/2021-09/21-07-27_opinion_enisa_transfers_third_countries_en.pdf.

⁵⁷ Similar to Article 49 of the GDPR.

⁵⁸ <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9668051> and <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9670061>

managing the App committed themselves to minimize user data collected for the purpose of activating the 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 user alerts from being disclosed to Google), 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 May 2021, the State Data Protection Authority for the German state of Baden-Württemberg has published a press release⁵⁹ advising against the use of a specifically configured version of Microsoft Office 365 at schools, as part of the education platform for schools in order to provide teachers, students and parents with a suitable digital infrastructure for teaching and education, due to high privacy risks and claimed that alternative solutions should be strengthened⁶⁰.

On 11 May 2021, based on a complaint, the PT SA issued a warning to a University, under Article 58(2) (a) of the GDPR on the likelihood that the data processing of its e-proctoring program infringes Article 5(1) (a) to (c) of the GDPR. The university had contracted the use of applications Respondus Lockdown Browser and Respondus Monitor as tools for monitoring examinations. Upon collection, the data was transferred to the US by AWS with no supplementary measures, pursuant to the Schrems II judgement. The PT SA also, under Article 58 (2)(d) of the GDPR, issued an order to delete data concerning staff and some students, who had already downloaded the software for training purposes before the exams, that had been transferred to the US.

In May 2021, the EDPS opened two investigations following the Schrems II judgment.⁶¹ 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.

The PT SA, within an investigation into a platform set up to follow Covid-19 patients under surveillance or self-care, called 'Trace Covid19', found out that the authentication services to gain access to the platform were provided by the health establishments but synchronised with the Microsoft Azure Active Directory. The PT SA verified that the contract required by Article 28 of the GDPR was a standard contract with no possibility for inserting tailor-made clauses suitable for the data processing. The PT

⁵⁹ <https://www.baden-wuerttemberg.datenschutz.de/lfdi-raet-aufgrund-hoher-datenschutzrechtlicher-risiken-von-der-nutzung-der-geprueften-version-von-microsoft-office-365-an-schulen-ab/>.

⁶⁰ According to the press release, « Controllers – and these are the schools (cf. Article 4 No. 7 GDPR) – do not have complete control over the overall system and the US processor in the chosen system. According to the assessment of the State Commissioner, they are currently unable to sufficiently understand which personal data are processed, how and for what purposes, and they cannot prove that the processing is reduced to the minimum necessary for this purpose. However, they would have to do all this in order to meet their accountability under Article 5 (2) GDPR. In addition, for some transfers of personal data to Microsoft – sometimes also in regions outside the EU – no legal basis is recognizable, which is required under the GDPR. This applies in particular to international data flows in the light of the Schrems II judgment of the European Court of Justice from 2020. [...] "It does not seem completely out of the question to work legally in the school sector with other variants of the products used in the pilot test and under significantly modified operating conditions. In recent months, however, it has not been possible to find such a solution, even after intensive cooperation and a high level of human resources." (unofficial translation)

⁶¹ https://edps.europa.eu/press-publications/press-news/press-releases/2021/edps-opens-two-investigations-following-schrems_en.

SA made a critical assessment of the situation and provided recommendations for the controller to comply with the GDPR and to put adequate contractual clauses in place.

After the "Schrems II" ruling, the FR SA has assisted the "Conférence des grandes écoles (CGE)" and the "Conférence des présidents d'université (CPU)" in the compliance with the GDPR of collaborative digital tools used in higher education and academic research that are provided by US companies. In its press release of May 2021⁶², the FR SA recognized that the risk of illegal access to this data by the US authorities must be excluded. However, considering the context of the health crisis, the need for the colleges and universities concerned to ensure the continuity of operations with the use of digital tools may have justified use during a transitional period. The FR SA committed itself to provide all the necessary assistance to these colleges and universities to identify possible alternatives during that transitional period. However, the FR SA reminded that *"The European Data Protection Board has still not identified any additional measures that would ensure an adequate level of protection when a transfer is made to a cloud computing service provider"*.

On 27 April 2021, following complaints, the PT SA issued an order under Article 58(2) (j) of the GDPR to suspend the data flows to the US or any other third country with no adequate protection, via Cloudflare, a company based in San Francisco, California, within 12 hours. The personal data at stake were contained in the replies provided by citizens to the National Statistics Institute. The contract between the controller and Cloudflare as processor was based on both the Privacy Shield (already invalidated by the CJEU) and SCCs with no supplementary measures adopted. The suspension was based on the Schrems II judgement.⁶³

In the Netherlands, in the first quarter of 2021 two parties submitted a DPIA to the NL SA about the (further) use of Google G Suite/Workspace after conducting a DPIA. Firstly, the Dutch Ministry of Justice and Security submitted a request for prior consultation about the possible deployment of Google G Suite Enterprise by Dutch government organisations. Secondly, SURF and SIVON⁶⁴ consulted the NL SA about the (further) use of Google G Suite Education. In short, the NL SA advised against the (further) use of Google G Suite/Workspace (for education) by both parties⁶⁵. This was mainly based on the high risks that were already identified in the DPIA. Among others, the outcome of the DPIA showed that there are fundamental issues relating to purpose limitation, transparency and the roles of the parties. With the advice of the NL SA, the negotiating parties reached an agreement with Google⁶⁶. The Ministry has stated that all high-risks are mitigated to such an extent that they are longer classified as 'high'.

⁶² CNIL calls for changes in the use of US collaborative tools by French universities, 31 May 2021, available at: <https://www.cnil.fr/en/cnil-calls-changes-use-us-collaborative-tools-french-universities>.

⁶³ Order of the PT SA, 27 April 2021, available at: <https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/121875>
<https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/121875>

⁶⁴ SURF is a cooperative association of Dutch education and research institutions in which the members (100+) join forces. SURF offers its members several IT services such as network connectivity, security, trust & identity, and also joint procurement of IT facilities and contract management. Sivon is also a cooperation, but with a focus on the primary and secondary educational sector. Both parties negotiate with CSPs on behalf of their members.

⁶⁵ Dutch Data Protection Authority on Google G Suite for Education, 08 June 2021, available at: <https://www.rijksoverheid.nl/ministeries/ministerie-van-onderwijs-cultuur-en-wetenschap/documenten/kamerstukken/2021/06/08/advies-autoriteit-persoonsgegevens-inzake-google-g-suite-for-education>.

⁶⁶ Letter to Parliament on data protection agreements between Google Workspace for Education, 8 July 2021, available at: <https://www.rijksoverheid.nl/documenten/kamerstukken/2021/07/08/kamerbrief-voortgang-advies-autoriteit-persoonsgegevens-inzake-google-g-suite-for-education>.

The NL SA also called upon the Dutch ministers for education, amongst others, to raise the issues on an EU level and start coordinated actions in order to safeguard person data in the context of cloud use for education.⁶⁷ In addition, SLM Rijk, which is a strategic vendor manager for public bodies in the Netherlands, had conducted several DPIAs on Microsoft and Google products on behalf of Dutch governmental organisations. The DPIAs are publicly available⁶⁸.

In the context of its Schrems II Strategy,⁶⁹ 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. The EDPS also strongly encouraged the EU institutions and bodies to avoid processing activities that involve transfers of personal data to the US. Following that order, the EDPS has received numerous requests for guidance on proper compliance, which it has provided as informal and formal supervisory opinions.

The EL SA examined ex officio the compliance of the Hellenic Ministry of Education and Religious Affairs on the compatibility of modern distance education in primary and secondary schools⁷⁰ -during the lockdown imposed due to the Covid -19 pandemic- with the provisions of the GDPR. In the context of the case, the updated DPIA and the compliance actions of the Ministry were examined. In September 2020, the EL SA identified five deficiencies, including that no proper evaluation of data transfer to non-EU countries had been carried out, in particular in the light of the Schrems II judgement after taking into account that the processor's parent company (Cisco Inc.) is established in the USA, and that Cisco universal cloud is being used. The EL SA reprimanded the Ministry for this violation and instructed the latter to address the deficiencies⁷¹ within 4 months. In 2022, the EL SA examined the Ministry's compliance with the above decision. It found that no further corrective measures were required and called on the Ministry to make the necessary amendments to improve transparency. In the decision, it is mentioned that the general issue of the application of Chapter V to videoconferencing services provided by companies – members of a group controlled by an entity subject to US law, will be examined with the other supervisory authorities through the cooperation and consistency procedures of the GDPR (Decision 61/2022⁷²).

On April 15, 2020, the Health Data Hub⁷³, a French public platform created in 2019 to share health data to support research projects concluded a contract with Microsoft. In an emergency procedure,

⁶⁷ https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/brief_minister_voor_basis-en voortgezet onderwijs_en_media.pdf

⁶⁸ <https://slmmicrosoftrijk.nl/downloads-dpias/>

⁶⁹ [EDPS Strategy for Union institutions, offices, bodies and agencies to comply with the 'Schrems II' Ruling](#), available at https://edps.europa.eu/sites/default/files/publication/2020-10-29_edps_strategy_schremsii_en_0.pdf

⁷⁰ EL SA Opinion 4/2020 on the compatibility of modern distance education in primary and secondary schools, 7 September 2020, available at: <https://www.dpa.gr/el/enimerwtiko/prakseisArxis/gnomodotisi-se-shesi-me-ti-syghroni-ex-apostaseos-ekpaideysi-stis>.

⁷¹ EL SA Decision 50/2021, 16 November 2021, available at: <https://www.dpa.gr/el/enimerwtiko/prakseisArxis/diadikasia-syghronis-ex-apostaseos-ekpaideysis-apo-ypoyrgeio-paideias>. See in particular paragraph 20

⁷² EL SA Decision 61/2022, 1 November 2022, available at: <https://www.dpa.gr/el/enimerwtiko/prakseisArxis/symmorfosi-toy-ypoyrgeioy-paideias-kai-thriskeymaton-me-tin-apofasi>

⁷³ CNIL, The Health Data Hub, 9 February 2021, available at: <https://www.cnil.fr/fr/la-plateforme-des-donnees-de-sante-health-data-hub>.

the Conseil d'État (High Administrative Court)⁷⁴ pointed out that Microsoft must refrain from transferring health data to the US. It acknowledged the risk of access by US authorities, but also that it did not justify, in the very short term, the suspension of the Hub because of the context of the health crisis and the necessity to ensure the continuity of the services offered by the Hub. The judge ordered the Health Data Hub to find a permanent solution that will eliminate any risk of access by US authorities. In accordance with the judge's request, the FR SA verified, for each request for authorization of research projects using the Health Data Hub, that the interest of the project, considering the health emergency of the Covid-19 pandemic, was sufficient to justify the risk incurred and that the use of the Hub was necessary.

In January 2020⁷⁵, 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.

In 2019-2020, the EDPS carried out an investigation into the use of Microsoft's products and services by EU institutions and bodies. On the basis of that investigation, the EDPS issued its Findings and Recommendations to the EU institutions and bodies.⁷⁶ 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.

Since 2019, there have been ongoing ministerial discussions in Estonia, led by the Ministry of Economic Affairs and Communications, to decide when the public sector, i.e., government and local government authorities can use cloud services. The discussions focus on workspace services (SaaS and Platform as a Service (PaaS) - e-mail, MS Office, Intranet platforms like Atlassian etc. Public sector official databases, registries are not under discussion.

⁷⁴ CNIL, The Conseil d'État asks the Health Data Hub for additional guarantees to limit the risk of transfer to the United States, 14 October 2020, available at: <https://www.cnil.fr/fr/le-conseil-detat-demande-au-health-data-hub-des-garanties-supplementaires>.

⁷⁵ <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9283857>

⁷⁶ See the EDPS Public Paper on the Outcome of own-initiative investigation into EU institutions' use of Microsoft products and services, available at https://edps.europa.eu/sites/default/files/publication/20-07-02_edps_paper_euis_microsoft_contract_investigation_en.pdf.

5 POINTS OF ATTENTION FOR PUBLIC BODIES

Following the completion of the analysis of the issues identified through the CEF Action, and the review of the SAs' decisions, this section of the report provides a list of points of attention that stakeholders can take into account when concluding agreements with CSPs, without prejudice to the provisions of the GDPR.

A non-exhaustive list of possible further actions by Supervisory Authorities is also presented.

Public bodies should consider the following, without prejudice to other GDPR provisions, when using cloud services, in order to ensure that their cloud implementation complies with GDPR:

- **Carry out a DPIA**, when it is necessary for the use of cloud services, in order to determine any necessary supplementary technical and organisational measures that would be required. If the DPIA is required and was not performed prior to the processing as required by Art 35 GDPR, notwithstanding the assessment of the public body's liability, the DPIA should be performed "ex post" as soon as possible, and the technical and organisational measures identified should be implemented.

A risk assessment should at the very least be undertaken, even if a DPIA is not legally required by the GDPR, in order to comply with Articles 24 and 32 of the GDPR. The processor should, if appropriate, provide assistance for the risk assessment, given that they may be in a better position to determine at least some of the organisational and technical measures. Only CSPs that offer sufficient guarantees should be selected.

- **Ensure that the roles of the involved parties are 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 or within the scope of a DPIA. 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.

- Ensure the **CSP acts only on behalf of and according to the documented instructions of the public body and identify any possible processing by the CSP as a controller**⁷⁷. Public bodies should identify clearly and assess the processing operations for which the CSP intends to act as a controller in order to ensure that there is always a valid legal basis for any communications of personal data to a CSP acting as a separate (or joint) controller. Besides, the CSP will have to ensure compliance with the GDPR, including by identifying a valid legal basis in relation to the specified, explicit and legitimate purposes for which personal data are processed.

- **Ensure that a meaningful way to object to new sub-processors is possible**, for instance by proposing a meaningful right to review a change of the list of relevant sub-processors and to transmit reasoned objections within a specified period in a way that it provides a meaningful right to object. In particular, it is important to review how and when public bodies can be informed about the specific sub-processors engaged in the processing activities⁷⁸, the criteria for appointing new/other sub-

⁷⁷ Although there can be situations in which a CSP is a controller, this should be an exception due to the fact that a processor should act on the documented instructions of the controller. This therefore cannot lead to a situation in which a public body who failed to do a proper risk assessment or negotiate a contract with a CSP hands over personal data from individuals to a CSP. Even in the exceptional situation in which a CSP subsequently processes personal data for a small number of purposes, the CSP will need, among others, a legal basis for the processing he is controller for. Also see art 6(4) GDPR

⁷⁸ Art. 28(2) GDPR provides that "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

processors, and under which provisions they can exercise their right to object according to Article 28(2) of the 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.

- **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, including by the CSP. This could be done by way of clear and exhaustive provisions⁷⁹ stipulated in **a contract concluded pursuant to Article 28 (3)** of the GDPR as well as organisational and technical measures, as necessary. The controller should adequately establish its role in the processing activities and its relationship with the CSP, while the contract could specify the security controls applied by the processor and the measures to be taken in order to mitigate the risks.

- **Promote the DPO's involvement** when determining or accepting the relevant clauses. The DPO should play an active role in the analysis and negotiation of contracts offered by CSPs.

- **Cooperate with other public bodies when negotiating with the CSPs.** It is a widespread impression among the SAs and 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. 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. Given the hyper-scale nature of some service providers, EU/EEA countries may also consider coordinating the procurement efforts of their public authorities to compensate the imbalance.

- Carry out a **review to assess if processing is performed in accordance with the DPIA** at least when there is a change of the risk represented by processing operations (Article 35 (11) of the GDPR). A switch to cloud may be the change of the risk that would need to entail a review of DPIA, and that a periodic review may be needed. It is necessary to **regularly review and re-assess** the DPIA (and/or the risk assessment), since cloud services are dynamic and continuously subject to change.

- **Ensure that the procurement procedure already envisages all the necessary requirements** to achieve compliance with the GDPR, preferably prior to the initiation of the procurement procedure itself.

- Identify which transfers may take place in the context of routine services provision, and in case of request of access to personal data by third country public authorities. Such transfers must comply with the provisions in Chapter V of the GDPR. **Public bodies should therefore provide instructions to the CSP in order to identify and use a proper transfer tool and, if necessary, to identify and implement appropriate supplementary measures.** A renegotiation of the contract to prevent or stop such transfers, or the use of another cloud solution compliant with the GDPR, may be needed (e.g. compliant EEA-sovereign cloud solutions).

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.”

⁷⁹ The standard contractual clauses on controller / processor can also be helpful as a guidance when drafting bespoke contracts in this type of relation. The EDPB has already issued opinions on the EU Commission SCC but also on SCC adopted by DK SA, SI SA, and LT SA. See [Opinions | European Data Protection Board \(europa.eu\)](#)

- **Analyse if a legislation of a third country would apply to the CSP and would lead to the possibility to address access requests to data stored by the CSP in the EEA⁸⁰.** Public bodies should therefore assess:

- 1) whether the contract provides for instructions to the CSP to process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the CSP is subject;
- 2) whether the CSP or its employees would be under the legal obligation to provide access to the data to third country public authorities and, if this is the case, would be under the legal obligation to maintain confidentiality, and would thus be prevented from informing the controller about them;
- 3) whether such access requests could be met in compliance with Article 48 (meaning with a valid legal basis and a valid ground for transfer);
- 4) whether the third country legislation provides for possible exemption/immunities for access requests concerning data processed by or on behalf of public authorities;
- 5) In particular, where no valid ways to answer the access requests would be identified, whether appropriate and proportionate technical, organisational, and/or legal safeguards according to Article 28 are in place or can be put in place⁸¹.

- **Examine closely and if necessary renegotiate the contract** with the CSP to ensure GDPR-compliance for all data processing involved, including regarding the lawfulness of processing of telemetry data.

- **Verify the conditions under which the public body is allowed for and can contribute to audits**, including inspections, conducted by the public body itself or another auditor mandated by the controller, and ensure that they are in place.

⁸⁰ It stems from the analysis led by the authorities that the sole use of a CSP that is part of a multinational group subject to third country laws may result in the concerned third country laws also applying to data stored in the EU. Possible requests might in this case be addressed directly to the CSP within the EU and would concern data present in the EU and not data already undergoing transfer. Public bodies/controllers in the EEA should therefore carry out a thorough assessment of cases where CSP in the EU/EEA could face access requests directly or indirectly from public authorities in third countries so that sufficient safeguards can be implemented. With respect to access by third country public authorities, a thorough analysis should be undertaken before the conclusion of the contract

⁸¹ Similar safeguards as those provided by the EDPB in the recommendations concerning supplementary measures for transfers could be adduced.

6 CONCLUSION

In order to ensure a GDPR compliant implementation of cloud services, public bodies should take their responsibilities to assess and where necessary renegotiate cloud contracts, with close involvement of the DPO.

The present report is the state of play, at the end of 2022, of the CEF action regarding the use of cloud by public bodies. It may need to be updated in the course of 2023 to take into account the progress of the procedures which have not yet been completed to date and given the issues identified, further complementary work on general recommendations to public actors concerning the use of cloud service providers could be foreseen.

While this report presents a number of leading practices and points of attentions for controllers using cloud services, SAs will also continue to promote compliance of cloud-based solutions, either because some of their investigations are still ongoing, or because they already envisage follow up actions.

This may include awareness raising campaigns via the publication of non-binding opinions (or recommendations) on the obligations of controllers using cloud services, on the importance of conducting a DPIA⁸², on the importance of signing a contract or other legal act that complies with the requirements of Article 28 (3) of the GDPR and/or on any other issues identified in this report.

Other follow-up actions may include further engaging with the public bodies/stakeholders and the CSPs concerned on the issues raised, including by setting up technical working groups, or finalising ongoing inspections, launching new investigations, and taking corrective measures where appropriate. The EDPB will also continue to raise awareness on leading practices regarding the use of cloud services.

Finally, SAs acknowledge the added-value of coordinated work under the CEF. The 2022 action has promoted a detailed and harmonised approach to GDPR compliance of products and services, relying on cloud-based solutions, by the national and EU public sector. Both the methodology and approach used for this CEF action will pave the way for more coordinated work by SAs on other topics, starting with the CEF 2023 action on the designation and role of the DPO.

⁸² and on already available guidance on this matter

ANNEX 1: DEFINITIONS

The following terminology which can be found in this document, is reused from [ISO 17788](#)⁸³

Cloud computing	Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.
Cloud service	One or more capabilities offered via cloud computing invoked using a defined interface.
Cloud service provider	Party which makes cloud services available
Infrastructure as a Service (IaaS)	Cloud service category in which the cloud capabilities type provided to the cloud service customer is an infrastructure capabilities type.
Platform as a Service (PaaS)	Cloud service category in which the cloud capabilities type provided to the cloud service customer is a platform capabilities type.
Software as a Service (SaaS)	Cloud service category in which the cloud capabilities type provided to the cloud service customer is an application capabilities type.
reversibility	Process for cloud service customers to retrieve their cloud service customer data and application artefacts and for the CSP to delete all cloud service customer data as well as contractually specified cloud service derived data after an agreed period.
private cloud	Cloud deployment model where cloud services are used exclusively by a single cloud service customer and resources are controlled by that cloud service customer
public cloud	Cloud deployment model where cloud services are potentially available to any cloud service customer and resources are controlled by the CSP
tenant	One or more cloud service users sharing access to a set of physical and virtual resources.
hybrid cloud	Cloud deployment model using at least two different cloud deployment models
community cloud	Cloud deployment model where cloud services exclusively support and are shared by a specific collection of cloud service customers who have shared requirements and a relationship with one another, and where resources are controlled by at least one member of this collection.

⁸³ ISO/IEC 17788: Information technology — Cloud computing — Overview and vocabulary