The EDPB provides for further guidance on the use of cloud solutions in line with the GDPR

In just a few years, the use of cloud services has increased significantly in both the public and private sectors. A trend that has been further accelerated by the Covid-19 pandemic and the drive for digital transformation across all sectors. This is not without risk from a data protection perspective, especially when it involves the (often-unavoidable) use of a hyper-scale Cloud Service Provider (CSP) which belongs to a group outside the EU/EEA. A number of recent publications by the European data protection board (EDPB) are of particular relevance in this context. Here is a summary of some of the main takeaways that have emerged from them:

State of play of the use of cloud solutions in the public sector: lessons to be learned for the private sector as well

In 2022, most data protection authorities in the EU started to carry out a so-called Coordinated Enforcement Action on the EU level pertaining to the use of cloud-based services by the public sector.

The EDPB has compiled the findings of the participating national supervisory authorities on the use of CSPs in the public sector following these coordinated investigations throughout 2022 and published a "state of the play" report on 17 January 2023. In particular, this report contains a list of points of non-compliance of several public sector actors across the EU when entering into agreements with CSPs.

These GDPR violations may be followed by corrective actions initiated by the different national data protection authorities. Luxembourg was one of the only countries which was not in the scope of this coordinated enforcement action but the report provides many insights that are not only useful for the public sector but for any organisation, thus also private sector actors, that deploys cloud services or intends to do so.

The report revealed, amongst others, that:
- often the obligatory **data protection impact assessments** (DPIAs) and/or involvement of the **DPO** are insufficient or sometimes even absent ;
- often the **roles and responsibilities of the client and the CSPs** are not (adequately) qualified, whereby the EDPB also indicated that "*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 GDPR*" ;
- often the **control on the sub-processing chain** is insufficient – indeed CSPs rely on a multitude of sub-contractors; as well as
- the collection and use of **telemetry/diagnostic information**.

The report included an inevitable point on international data transfers and the consequences of the Schrems II ruling of the Court of Justice of the European Union in July 2020: a difference seems to be made between the scenario where the regular provision of cloud services entails quasi automatically an international data transfer (e.g., access for maintenance and support) and the scenario where this is not the case but where there could be a potential 3rd country governmental access.

In that last case, the focus does not seem to lie on Chapter V GDPR on international data transfers (as long as the there is no actual transfer) but rather on the requirement that data processors must be choses offering sufficient security measures (incl. against unauthorised access).

However, in the first scenario and where there is an actual international transfer, the report states that "[…] *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 controller to identify different solutions in order to prevent or stop such transfers e.g., by (re)negotiating contracts or using different cloud solutions which are compliant to the GDPR (e.g. compliant EEA-sovereign cloud solutions)*".

As recommended by the EDPB, to avoid such time-consuming negotiations with CSPs or a change of solution along the way, the EDPB recommends for public bodies to the extent possible to "*ensure that the procurement procedure already envisages all the requirements to achieve compliance with the GDPR, preferably before the initiation of the procurement procedure itself*". Based on our experience, we see that there is an increasing interest in the matter: where public sector players do not limit the risk of non-compliance with the GDPR provisions on international data transfers in tenders with a cloud element, this may lead to litigation when a competitor deems that the winning candidate does not comply with these provisions.

We have also seen that the public sector, in the Netherlands for example, has carried out extensive DPIAs and has forced undertakings such as Microsoft and Zoom to amend some of their practices.

The overview of actions that have been undertaken by the different authorities on the use of cloud solutions in the public sector (pp. 21-30), is certainly worth a close reading and will be most instructive for private sector entities as well.

Obligations arising from the use of a CSP subject to 3rd country legislation

In order to limit the risk of personal data being transferred to a third country, it is not uncommon for a private or public entity to engage an EU/EEA entity of a CSP on the condition that the data are hosted in the EU/EEA and that no one outside the EU/EEA, including its (often US) parent company nor its subcontractors, has access to the data.

Data hosted by the EU/EEA entity of a CSP that belongs to a group outside the EU/EEA may nevertheless be accessed by 3rd country enforcement agencies under certain circumstances. For example, it is not excluded that data hosted in the EU/EEA by Luxembourg-based CSP Amazon Web Services EMEA s.à r.l. can be accessed if its mother company Amazon Web Services, Inc. is subject to a request from the US enforcement authorities to produce data in the course of a specific criminal investigation under the so-called CLOUD Act.

Some data protection authorities have tried in the past to argue that the mere possibility to produce data under the CLOUD Act already triggered in itself the GDPR provisions on international data transfers.

In the latest version 2.0 of its guidelines 05/2021 on the interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR adopted on 14 February 2023, the EDPB confirmed – implicitly but unambiguously – its position that could already be inferred from its report on the state of the play of the Coordinated Enforcement Action on EU level pertaining to the use of cloud-based services by the public sector: until such request does not materialise, there is no transfer and the GDPR provisions on international data do not apply. However, if such a request is addressed to the CSP and the latter complies with this request, the disclosure is to be considered a transfer under Chapter V of the GDPR carried out in violation of the controller's instructions.

In this regard, the EDPB recalls that it is up to the controller to ensure, before engaging the CSP, that the latter provides as data processor sufficient guarantees to implement appropriate technical and organisational measures to comply with the GDPR as required by Article 28 GDPR. Those guarantees should also have regard to reliability, "*which may be in doubt if the processor is subject to third country legislation which may prevent it from fulfilling its obligations as a processor*". Such measures may include, for instance, a commitment by the data controller to contest the access request to the maximum extent permitted by applicable foreign law or to grant access to data only in an anonymous form.

In its decision of 31 January 2023, the Conference of German DPAs has taken a similar stance and put the bar quite high for those guarantees to be sufficient and seems to follow a quasi zero-risk approach via Article 28 GDPR. However, we believe that "*appropriate technical and organisational measures*" in Article 28 GDPR echoes the requirement laid down in Article 32 GDPR. This provision requires that the controller and the processor must implement "*appropriate technical and organisational measures*" and this "*to ensure a level of security appropriate to the risk*", whereby the "risk" is to be assessed in the light "*of varying likelihood and severity for the rights and freedoms of natural persons*".

In other words, if there is no actual transfer of personal data outside the EU/EEA, a risk-based approach must be possible, taking into account cases where there is rather a low risk that personal data will be the object of a measure of mass surveillance (of course there will be cases where that risk is higher) or any other non-compliant 3rd country governmental agency disclosure request.

What about personal data transfers to the US?

On 28 February 2023, the EDPB issued its opinion on the European Commission draft adequacy decision relating to the EU-US data privacy framework (DPF). The DPF is designed to replace the previous framework, known as the "Privacy Shield", which was struck down by the Court of Justice of the European Union (CJUE) on 16 July 2020 in the famous Schrems II case.

In essence, the CJEU identified several shortcomings in US national security legislation, allowing for far-reaching (*i.e.* not limited to what is strictly necessary and proportional) possibilities of surveillance by US authorities, which impede personal data protection and violate the GDPR. In particular, the CJEU found that the US law did not provide data subjects with rights that could be enforced before an independent and impartial court against the US authorities.

This has a significant impact on US-based CSPs and their subsidiaries in Europe, which had to find a new way to legitimise their data transfers under Chapter V of the GDPR. Most of them have therefore opted for the use of the European Commission's standard contractual clauses (SCCs), which have been updated as of 4 June 2021 as a result of the Schrems II ruling. However, to ensure that the US legislation does not affect the level of protection afforded by the SCCs in a way that would render them ineffective, the concerned data controllers and the CSPs had to take additional supplementary measures (especially in terms of pseudonymisation and encryption) to accompany these clauses. As set forth above under **1.**, the EDPB and the national data protection authorities are quite pessimistic as to whether there can be supplementary measures that would be sufficient to stop US authorities from accessing data.

The DPF is therefore a response to the deficiencies of the previous "Privacy Shield" and also to the lack of effective supplementary measures when SCCs are used.

As was the case before, the DPF will only apply to US organisations that have self-certified to the requirements of the framework. However, in contrast to the previous one, this new framework will be based on the additional safeguards laid down in Executive Order 14086 on enhancing safeguards for united states signals intelligence activities (EO 14086) issued by the US President on 7 October 2022 following negotiations with the European Commission. EO 14086's key innovations include:
- the introduction of the concepts of necessity and proportionality in the US intelligence legal framework in the form of a list of purposes for which data collection may or may not take place; as well as
- the establishment of an independent Data Protection Review Court (DPRC), which is empowered to hear complaints from EU individuals and to issue binding decisions to remedy covered violations (*e.g.* deletion of unlawfully collected data).

While the EDPB welcomes those "*substantial improvements*", it nevertheless expresses concerns regarding their effectiveness. Without going into details, the list of objectives for which a collection of data is allowed could be updated with additional and not necessarily public objectives in the light of new national security imperatives.

As far as the DPRC is concerned, in order to avoid revealing whether or not the complainant was subject to US signals intelligence activities, the latter will simply be notified that either no covered violations were identified or that a determination requiring appropriate remediation was issued, this standard response being not subject to appeal. For this reason, the EDPB asks the European Commission to closely monitor the practical functioning of this mechanism.

There have, of course, been a number of other recommendations made to the European Commission with regard to the review of the adequacy decision. Some of them are similar to those formulated by the LIBE Committee in the European Parliament in its resolution of 14 February 2023 calling for the outright rejection of the draft DPF and the continuation of negotiations with the Commission's US counterparts.

Even when the EDPB opinion sounded less dramatic than the LIBE Committee resolution, it is by no means certain that the DPF will be adopted in its current form in the near future or will stand the test in a potential Schrems III case. This means that US-based CSPs and their subsidiaries in the EU/EEA will have to continue to use another other legal basis provided for in Chapter V of the RGPD, SCCs, and supplementary measures in particular, for a while.

In light of the foregoing, there is no doubt that private and public sector actors need to pay particular attention to the choice of their CSPs, especially if there are subject to the law of a third country with extraterritorial effects such as the US surveillance legislation. In this respect, public bodies should make the most of their advantage of being able to formulate their requirements in advance of the tendering process in order to ensure the compliance of their data processing with the GDPR, including with respect to international transfers.

Vincent WELLENS (portrait)
Avocat à la Cour (Luxembourg) / Avocat (Bruxelles)
Partner NautaDutilh Avocats Luxembourg S.à r.l.
vincent.wellens@nautadutilh.com

Antoine PETRONIN
Avocat (Luxembourg)
Associate NautaDutilh Avocats Luxembourg S.à r.l.
antoine.petronin@nautadutilh.com