New guidance on the use of cloud services

The data protection rules do not specify what technologies an organisation may use to process personal data, as the rules are technology-neutral. However, some technologies present more challenges than others.

In the light of the Schrems II decision and the subsequent decisions of the Austrian and French Data Protection Authorities concerning the use of Google Analytics, there has been some uncertainty about the use of cloud services. Therefore, the Danish Data Protection Agency has now published new guidance to help organisations that use or intend to use cloud services. At the same time, cloud service providers will have the opportunity to learn how they can provide services in accordance with data protection rules. The guide is also available in English.

CONTENT OF THE GUIDE

In addition to a detailed review of the different kinds of cloud services you as an organisation can choose from, the guidance contains a review of the considerations you should make when choosing a cloud solution as well as a number of practical recommendations.

KNOW YOUR SERVICES AND SUPPLIERS

Under the data protection rules, it is a fundamental requirement that you as a data controller have an overview of what personal data is processed, for what purposes they are processed, and how they are processed. This is necessary to carry out the required risk assessments.

The guidance provides several questions that should be answered in the context of the required risk assessments of data protection and the level of security. It is important to point out that these risk assessments must be made regardless of whether you use cloud providers or not, but that such use will add more factors to the risk assessments.

The guidance indicates that a controller should ask these questions in the context of the data protection risk assessment:

1. Does the cloud provider process additional personal data than the personal data entrusted to the cloud provider? For example, metadata or other service data.
2. Does the cloud provider process the personal data transferred to the cloud provider for its own purposes? If so, a legal basis must be found.

Also, the guidance indicates that the data controller should determine the supplier's level of security and assess whether this level of security is appropriate for its risk assessment.

In addition, the guidance lists a number of questions that the data controller should ask when screening cloud providers and provides an in-depth explanation of the key points.

SUPERVISION OF THE CLOUD PROVIDER AND ANY SUBCONTRACTORS

The Danish Data Protection Agency also elaborates on the requirements for the supervision of data processors and sub-processors in relation to cloud providers. This must be done in addition to the requirements that exist for the supervision of data processors, which you can read more about in the Danish Data Protection Agency's guidance on supervision of data processors.

The guidance states that the controller should review the audit report (where available). Still, it is necessary to be aware of whether the audit report relates to the processing activities carried out by the cloud provider for the controller.

In the absence of relevant audit reports, the controller shall ensure that they are entitled to require an audit of the processing operations.

TRANSFERS TO THIRD COUNTRIES, INCLUDING THE UNITED STATES

The new guidance underlines the previous announcements from the Danish Data Protection Agency regarding transfers to third countries and additional measures.

The most important thing to be aware of in connection with the use of cloud services outside the EU/EEA (third countries) is the Transfer Impact Assessment (TIA) to be prepared and the assessment of whether additional measures should be introduced. The TIA assessment is relatively new and has been introduced on the basis of the Schrems II decision. The guidance merely emphasises that the procedure laid down in the Danish Data Protection Agency's "Guidance on the transfer of persons to third countries" and the recommendations from the EDPB must continue to be followed.

However, the guidance also touches on the particular challenge of transfers of personal data to the United States, which has been raised by Schrems II and, in particular, by the new decisions from Austria and France on Google Analytics.

The Danish Data Protection Agency mentions that effective additional technical measures must be implemented in cases where a cloud provider in the USA is covered by FISA 702, which they most often are. However, the Danish Data Protection Agency stresses that if such a cloud provider has access to personal data in plain text, the Danish Data Protection Agency cannot at this time provide any additional technical measures that can be considered effective.

In addition, the Danish Data Protection Agency states in the guidelines that it is necessary for the data controller to be aware of whether cloud providers located within the EU/EEA may be met with requests for access to personal data from a third country. This may, for example, be on the basis of the cloud provider's group structure, where the parent company is established in a third country. This will be the case, for example, for U.S. cloud providers under the U.S. Cloud Act. In the opinion of the Danish Data Protection Agency, such a transfer to the authorities of a third country would be a breach of personal data security.

NJORD'S COMMENTS

Although the Danish Data Protection Agency's new guidance on the use of cloud services goes far and wide around the challenges associated with their use, we must note that it does not bring much new. Users of cloud services in third countries, including in particular the United States, continue to face the same challenges concerning the transfer of personal data outside the EU/EEA, and the guidance does not provide a real solution to this.

NIS PETER DALL
ATTORNEY AT LAW,
PARTNER

(+45) 77 40 10 18
NPD@NJORDLAW.COM

PERNILLE KIRK ØSTERGAARD
ATTORNEY AT LAW, SENIOR
SPECIALIST

(+45) 77 40 11 74
POS@NJORDLAW.COM