# ANNEX 2

## GUIDELINES – BEST PRACTICES WP29 AND DDPA

### Introduction

1. In this Annex we provide an overview of the guidelines and best practices as submitted by the Working Party on the Protection of Individuals with regard to the Processing of Personal Data ("WP29") and the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*). Special emphasis is laid on the contractual arrangements that should regulate the relationship between a controller and a processor in this connection.

### WP29

2. The opinion of The EU Data Protection Authorities, united in the Working Party on the Protection of Individuals with regard to the Processing of Personal Data ("WP29") analyses the obligations for controllers in the European Economic Area ("EEA") and for cloud service providers with clients in the EEA regarding cloud computing.[1] The relevant legal framework in this regard is the GDPR. The GDPR applies in every case where personal data are being processed as a result of the use of cloud computing services.

3. Although the WP29's opinions and guidelines are not binding, since it is an advisory body made up of a representative from the data protection authority of each EU Member State, and includes the European Data Protection Supervisor and the European Commission, these guidelines can assist in understanding how European data protection authorities will interpret various requirements of the GDPR.

4. The WP29 emphasizes that "in the current cloud computing scenario, clients of cloud computing services may not have room for manoeuvre in negotiating the contractual terms of use of the cloud services as standardised offers are a feature of many cloud computing services. Nevertheless, it is ultimately the client who decides on the allocation of part or the totality of processing operations to cloud services for specific purposes; the cloud provider's role will be that of a contractor vis-à-vis the client, which is the key point in this case. […] the imbalance in the contractual power of a small controller with respect to large 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. For this reason, the

[1] Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing, 1 July 2012, WP196.

controller must choose a cloud provider that guarantees compliance with data protection legislation. Special emphasis must be placed on the features of the applicable contracts – these must include a set of standardised data protection safeguards including […] – as well as on additional mechanisms that can prove suitable for facilitating due diligence and accountability."[2]

*Controller / processor*

5. Cloud computing involves particular two different players. It is important to assess and clarify the role of each of these players in order to establish their specific obligations with regard to data protection legislation. According to the WP29, the cloud provider can be considered a data processor while the client should be considered the controller:

> *The cloud client determines the ultimate purpose of the processing and decides on the outsourcing of this processing and the delegation of all or part of the processing activities to an external organisation. The cloud client therefore acts as a data controller. The cloud provider is the entity that provides the cloud computing services in the various forms discussed above. When the cloud provider supplies the means and the platform, acting on behalf of the cloud client, the cloud provider is considered as a data processor.*[3]

*Contractual safeguards*

6. Where controllers decide to contract cloud computing services, they are required to choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

7. The contract must at a minimum establish the fact, in particular, that the processor is to follow the instructions of the controller and that the processor must implement technical and organizational measures to adequately protect personal data. To ensure legal certainty the contract should also set forth the following issues:[4]

   i. *Details on the (extent and modalities of the) client's instructions to be issued to the provider, with particular regard to the applicable SLAs (which should be objective and measurable) and the relevant penalties (financial or otherwise including the ability to sue the provider in case of non-compliance).*

   ii. *Specification of security measures that the cloud provider must comply with, depending on the risks represented by the processing and the nature of the data to be protected. It is of great importance that concrete technical and organizational measures are specified such as those outlined below.*

---

[2] Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing, 1 July 2012, WP196, p. 8.
[3] Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing, 1 July 2012, WP196, p. 7-8.
[4] Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing, 1 July 2012, WP196, p. 13-14.

iii. *Subject and time frame of the cloud service to be provided by the cloud provider, extent, manner and purpose of the processing of personal data by the cloud provider as well as the types of personal data processed.*

iv. *Specification of the conditions for returning the (personal) data or destroying the data once the service is concluded. Furthermore, it must be ensured that personal data are erased securely at the request of the cloud client.*

v. *Inclusion of a confidentiality clause, binding both upon the cloud provider and any of its employees who may be able to access the data. Only authorized persons can have access to data.*

vi. *Obligation on the provider's part to support the client in facilitating exercise of data subjects' rights to access, correct or delete their data.*

vii. *The contract should expressly establish that the cloud provider may not communicate the data to third parties, even for preservation purposes unless it is provided for in the contract that there will be subcontractors. The contract should specify that subprocessors may only be commissioned on the basis of a consent that can be generally given by the controller in line with a clear duty for the processor to inform the controller of any intended changes in this regard with the controller retaining at all times the possibility to object to such changes or to terminate the contract. There should be a clear obligation of the cloud provider to name all the subcontractors commissioned (e.g., in a public digital register). It must be ensured that contracts between cloud provider and subcontractor reflect the stipulations of the contract between cloud client and cloud provider (i.e. that sub-processors are subject to the same contractual duties than the cloud provider). In particular, it must be guaranteed that both cloud provider and all subcontractors shall act only on instructions from the cloud client. As explained in the chapter on sub-processing the chain of liability should be clearly set in the contract. It should set out the obligation on the part of the processor to frame international transfers, for instance by signing contracts with subprocessors, based on the 2010/87/EU standard contractual clauses.*

viii. *Clarification of the responsibilities of the cloud provider to notify the cloud client in the event of any data breach which affects the cloud client's data.*

ix. *Obligation of the cloud provider to provide a list of locations in which the data may be processed.*

x. *The controller's rights to monitor and the cloud provider's corresponding obligations to cooperate.*

xi. *It should be contractually fixed that the cloud provider must inform the client about relevant changes concerning the respective cloud service such as the implementation of additional functions.*

xii. *The contract should provide for logging and auditing of relevant processing operations on personal data that are performed by the cloud provider or the subcontractors.*

xiii. *Notification of cloud client about any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.*

xiv. *A general obligation on the provider's part to give assurance that its internal organisation and data processing arrangements (and those of its sub-processors, if any) are compliant with the applicable national and international legal requirements and standards.*

*Technical and organisational measures of data protection and security*

8. The GDPR puts full responsibility on cloud clients (acting as data controllers) to choose cloud providers that implement adequate technical and organisational security measures to protect personal data and to be able to demonstrate accountability. The goals of data security are availability, integrity, confidentiality, transparency, isolation, intervenability, portability and accountability.[5]
    - Availability: it should be checked whether the (public) cloud provider has adopted reasonable measures to cope with the risk of disruptions, such as backup internet network links, redundant storage and effective data backup mechanisms.
    - Integrity: Interference with the integrity of IT systems in the cloud can be prevented or detected by means of intrusion detection / prevention systems (IPS / IDS).
    - Confidentiality: Communications between cloud provider and client as well as between data centres should be encrypted. Remote administration of the cloud platform should only take place via a secure communication channel. If a client plans to not only store, but also further process personal data in the cloud (e.g., searching databases for records), he must bear in mind that encryption cannot be maintained during processing of the data (except of very specific computations).
    - Transparency: The cloud client is only capable of assessing the lawfulness of the processing of personal data in the cloud if the provider informs the client about all relevant issues. A controller contemplating engaging a cloud provider should carefully check the cloud provider's terms and conditions and assess them from a data protection point of view. Technical and organisational measures must support transparency to allow review.
    - Isolation: Achieving isolation first requires adequate governance of the rights and roles for accessing personal data, which is reviewed on a regular basis. The implementation of roles with excessive privileges should be avoided (e.g., no user or administrator should be authorised to access the entire cloud). More generally, administrators and users must only be able to access the information that is necessary for their legitimate purposes (least privilege principle).
    - Intervenability: The contract between the controller and the cloud provider should stipulate that the cloud provider is obliged to support the controller in facilitating exercise of data subjects' rights and to ensure that the same holds true for his relation to any subcontractor.
    - Portability: If a cloud client decides to migrate from one cloud provider to another, lack of interoperability may result in the impossibility or at least difficulties to transfer

[5] Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing, WP 196, 1 July 2012, p. 14-15.

the client's (personal) data to the new cloud provider (so-called vendor lock-in). It must be verified whether and how the provider guarantees the portability of data and services prior to ordering a cloud service. Preferably, the provider should make use of standardised or open data formats and interfaces. In any event, contractual clauses stipulating assured formats, preservation of logical relations and any costs accruing from the migration to another cloud provider should be agreed on.

- Accountability: Cloud providers should provide documentary evidence of appropriate and effective measures that deliver the outcomes of the data protection principles outlined in the previous sections. Procedures to ensure the identification of all data processing operations, to respond to access requests, the allocation of resources including the designation of data protection officers who are responsible for the organisation of data protection compliance, or independent certification procedures are examples of such measures. In addition, controllers should ensure that they are prepared to demonstrate the setting up of the necessary measures to the competent supervisory authority upon request.

*International transfers*

9. The GDPR provides for free flow of personal data to countries located outside the EEA only if that country or the recipient provides an adequate level of data protection.[6] Otherwise specific safeguards must be put in place by the controller and its processors.[7]

10. Cloud customers should ask a potential cloud provider for a list of countries where data is likely to be processed and for information relating to the safeguards in place there. The cloud provider should be able to explain when data will be transferred to these locations.

11. In the case of layered cloud services, information relating to the location of each sub-processor involved in the processing of the data should also be available from the cloud provider, with details of the security arrangements in place.

**The Dutch Data Protection Authority (The Netherlands)**

12. The Dutch Data Protection Authority (*Autoriteit Persoonsgegevens)* has published a practical guide for the storage of medical patient data in the cloud and the way in which the controller must choose the right cloud provider.[8] This guide is also not binding, but can assist in

[6] Article 45 GDPR.
[7] Article 46 GDPR.
[8] Practical guide patient data in the cloud, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/praktijkgids_patientgegevens_in_de_cloud_def.pdf, accessed on 22 March 2018.

understanding how the Dutch Data Protection Authority will interpret the requirements of the GDPR.

13. The Data Protection Authority provides the following rules:
    - Risk analysis: the controller must carry out a risk analysis before transferring the data to the cloud. On the basis of this analysis the controller can know which risk are present. This risk analysis must be regularly updated.
    - Certification: the controller should check whether the cloud provider has a certification. Such a certificate proves that the cloud provider meets relevant practice standard. Different standards exist for the use of cloud services. The most relevant standards are ISAE 3402, ISO 27017 and NEN 7510. In addition, the general safety standards ISO 27001 and ISO 27002 also play a role.
    - Audit: a certificate is not mandatory. The reliability of a cloud provider can also be reflected in an audit report.
    - Access: the controller should check whether it always has and will have access to the data (also in case of bankruptcy). The controller should also make arrangements regarding the return of data (portability) in case of termination of the agreement.

14. With regard to the security of personal data in the cloud, the Data Protection Authority states the following:
    - the cloud provider may only process the personal data on behalf of the controller;
    - the cloud provider is not allowed to do anything on its initiative with that data;
    - the cloud provider has a duty of confidentiality;
    - the controller must ensure that the cloud provider implements proper security measures;
    - the controller must check whether the data is completely separated from the data of other customers of the cloud provider.

15. Attached is a document (in Dutch) submitted by the Dutch Data Protection Authority, providing guidelines concerning the protection of personal data.[9]

[9] Dutch Data Protection Guidelines Security of Personal Data, February 2013, https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf.