# Cloud Computing
# A guide for data controllers

Summary of the Article 29 Working Party Opinion
(amended to apply to Jersey and Guernsey Law)

This guidance relates to both the Data Protection (Jersey) Law 2005 and the Data Protection (Bailiwick of Guernsey) Law, 2001.

Where the Laws differ and to show differences between the two jurisdictions the page will be split as shown below.

| Jersey | Guernsey |
| --- | --- |
| Commissioner = Information Commissioner | Commissioner = Data Protection Commissioner |
| a = article within the Law | s = section of the Law |

Where numbering of passages from the Laws are the same it will be shown as a/s.

April 2016

# Table of Contents

# Heading

# Introduction

The Article 29 Working Party ("WP29") is made up of representatives from the Data Protection Authorities of each EU Member State, together with the European Data Protection Supervisor and the European Commission. Its main role is to give expert advice to Member States (and beyond) regarding specific aspects of data protection compliance and regulation, including the promotion of the application of the European Data Protection Directive and providing formal opinions to the European Commission on technological advances which may affect the right to protection of personal data.

On 1 July 2012, WP29 published an opinion on cloud computing, concentrating largely on the relationship between this technological advancement and the application of the European Data Protection Directive, upon which all EU domestic data protection legislation is based. The Commissioner for Jersey and Guernsey has adapted this opinion as a model for guidance to Jersey and Guernsey data controllers considering the use of cloud computing services.

The guidance outlines how the wide scale deployment of cloud computing services can trigger a number of data protection risks, mainly a lack of control over personal data as well as insufficient information with regard to how, where and by whom the data is being processed/sub-processed. These risks need to be carefully assessed by public bodies and private enterprises when they are considering engaging the services of a cloud provider.

A key conclusion of the WP29 opinion is that businesses and administrations wishing to use cloud computing should conduct, as a first step, a comprehensive and thorough risk analysis. Security, transparency and legal certainty for the clients should be key drivers behind the offer of cloud computing services.

It is thus recommended that the client should select a cloud provider that guarantees compliance with EU data protection legislation. Appropriate contractual safeguards are addressed in the opinion with the requirement that any contract between the cloud client and cloud provider should afford sufficient guarantees in terms of technical and organisational measures. Also of significance is the recommendation that the cloud client should verify whether the cloud provider can guarantee the lawfulness of any cross-border international data transfers.

# Key Risks

The majority of these risks fall within two broad categories namely lack of control over the data, and insufficient information regarding the processing operation itself (absence of transparency).

- Cloud providers process personal data emanating from a wide range of sources in terms of data subjects and organisations and it is a possibility that conflicting interests and/or different objectives might arise.

- Personal data being processed in the cloud may be subject to law enforcement requests from law enforcement agencies of the EU Member States and of third countries. There is a risk that personal data could be disclosed to (foreign) law enforcement agencies without a valid EU legal basis and thus a breach of EU data protection law would occur.

- The cloud service offered by one provider might be produced by combining services from a range of other providers, which may be dynamically added or removed during the duration of the client's contract.

- A cloud provider may not provide the necessary measures and tools to assist the controller to manage the data in terms of, e.g., access, deletion or correction of data.

- Insufficient information about a cloud service's processing operations poses a risk to controllers as well as to data subjects because they might not be aware of potential threats and risks and thus cannot take measures they deem appropriate.

- Some potential threats may arise from the controller not knowing that

    - Chain processing is taking place involving multiple processors and subcontractors.
    - Personal data are processed in different geographic locations within the EEA. This impacts directly on the law applicable to any data protection disputes which may arise between user and provider.
    - Personal data is transferred to third countries outside the EEA. Third countries may not provide an adequate level of data protection and transfers may not be safeguarded by appropriate measures (e.g., standard contractual clauses or binding corporate rules) and thus may be illegal.

It is a requirement that data subjects whose personal data are processed in the cloud are informed as to the identity of the data controller and the

purpose of the processing (an existing requirement for all controllers under Data Protection Directive 95/46/EC). Given the potential complexity of processing chains in a cloud computing environment, in order to guarantee fair processing in respect of the data subject (Article 10 of Directive 95/46/EC), controllers should also as a matter of good practice provide further information relating to the (sub-)processors providing the cloud services.

## Legal framework

The relevant legal framework is the Data Protection Law. The Law applies in every case where personal data are being processed as a result of the use of cloud computing services.

The criteria for establishing the applicability of legislation are contained in a/s 5 of the Law, which refers to the law applying to controllers with one or more establishments within the Island and also to the law applying to controllers who are outside the Island but use equipment located within the Island to process personal data.

In the first case, the factor that triggers the application of the Law to the controller is the location of his or her establishment and the activities it carries out, according to a/s 5 of the Law, with the type of cloud service model being irrelevant. The applicable legislation is the law of the country in which the controller contracting the cloud computing services is established, rather than the place in which the cloud computing providers are located.

A/S 5 also refers to how data protection legislation applies to controllers who are not established in the Island but use automated or non-automated equipment located in the territory of a Member State, except where these are used only for purposes of transit. This means that if a cloud client is established outside the Island, but commissions a cloud provider located in the EEA, then the provider exports the data protection legislation to the client.

## Duties and responsibilities of different players

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 client, as controller, must accept responsibility for abiding by data protection legislation and is responsible and subject to all the legal duties that are addressed in the Law. The cloud client may task the cloud provider with choosing the methods and the technical or organisational measures to be used to achieve the purposes of the 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 i.e., according to the Law "*any person who processes personal data on behalf of the controller, but does not include an employee of the data controller"*.

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 Article 29 Working Party ("WP29") Opinion 1/2010 (when discussing the concepts of controller and processor) states: *"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 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 as well as additional mechanisms that can prove suitable for facilitating due diligence and accountability (such as independent third-party audits and certifications of a provider's services).

## Subcontractors:

Cloud computing services may entail the involvement of a number of contracted parties who act as processors. It is also common for processors to subcontract additional sub-processors which then gain access to personal data. If processors subcontract services out to sub-processors, they are obliged to make this information available to the client, detailing the type of service subcontracted, the characteristics of current or potential sub-contractors and guarantees that these entities offer to the provider of cloud computing services to comply with the Law.

All the relevant obligations must therefore apply also to the sub-processors through contracts between the cloud provider and subcontractor reflecting the stipulations of the contract between cloud client and cloud provider.

In such scenarios, the obligations and responsibilities deriving from data protection legislation should be set out clearly and not dispersed throughout the chain of outsourcing or subcontracting, in order to ensure effective control over and allocate clear responsibility for processing activities.

A possible model of assurances that can be used to clarify the duties and obligations of processors when they subcontract data processing was first introduced by the European Commission Decision of 5 February 2010 on the standard contractual clauses for the transfer of personal data to processors established in third countries. In this model sub-processing is permitted only with the prior written consent of the controller and with a written agreement imposing the same obligations on the sub-processor as are imposed on the processor. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the processor shall remain fully liable to the controller for the performance of the sub-processor's obligations under such agreement. A provision of this kind could be used in any contractual clauses between a controller and a cloud service provider, where the latter intends to provide services through subcontracting, to assure required guarantees for the sub-processing.

The Commissioner concurs with the view of the WP29, that the processor can subcontract its activities only on the basis of the consent of the controller, which may be generally given at the beginning of the service with a clear duty for the processor to inform the controller of any intended changes concerning the addition or replacement of subcontractors, 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. In addition, a contract should be signed between cloud provider and subcontractor reflecting the stipulations of the contract between cloud client and cloud provider. The controller should be able to avail of contractual recourse possibilities in case of breaches of contracts caused by the sub-processors. This could be arranged by ensuring that the processor is directly liable toward the controller for any breaches caused by any sub-processors he has enlisted, or through the creation of third party beneficiary right for the benefit of the controller in the contracts signed between the processor and the sub-processors or by the fact that those contracts will be signed on behalf of the data controller, making this later a party to the contract.

# Data Protection requirements in the Client-Provider relationship

The lawfulness of the processing of personal data in the cloud depends on the adherence to basic principles of the Law: Namely, transparency vis-à-vis the data subject is to be guaranteed, the principle of purpose specification and limitation must be complied with and personal data must be erased as soon as their retention is not necessary any more. Moreover, appropriate technical and organisational measures must be implemented to ensure an adequate level of data protection and data security.

Transparency is of key importance for a fair and legitimate processing of personal data (1st Data Protection Principle). The Law obliges the cloud client to provide a data subject from whom data relating to himself are collected with information on his identity and the purpose of the processing. The cloud client should also provide any further information such as on the recipients or categories of recipients of the data, which can also include processors and sub-processors in so far as such further information is necessary to guarantee fair processing in respect of the data subject.

The principle of purpose specification and limitation requires that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes (2nd Data Protection Principle). The cloud client must determine the purpose(s) of the processing prior to the collection of personal data from the data subject and inform the data subject thereof. The cloud client must not process personal data for other purposes that are not compatible with the original ones.

Moreover, it must be ensured that personal data are not processed for further purposes by the cloud provider or one of his subcontractors. As a typical cloud scenario may easily involve a larger number of subcontractors, the risk of processing of personal data for further, incompatible purposes must therefore be assessed as being quite high. To minimise this risk, the contract between cloud provider and cloud client should include technical and organisational measures to mitigate this risk and provide assurances for the logging and auditing of relevant processing operations on personal data that are performed by employees of the cloud provider or the subcontractors. Penalties should be imposed in the contract against the provider or subcontractor if data protection legislation is breached.

Personal data must be kept for no longer than is necessary for the purposes for which the data were collected (5th Data Protection Principle).

Personal data that are not necessary any more must be erased or anonymised. If this data cannot be erased due to legal retention rules (e.g., other statutory requirements), access to this personal data should be blocked. It is the cloud client's responsibility to ensure that personal data are erased as soon as they are not necessary in the aforementioned sense any more. The principle of erasure of data applies to personal data regardless of whether they are stored on hard drives or on other storage media (e.g., backup tapes). Since personal data may be kept redundantly on different servers at different locations, it must be ensured that each instance of them is erased irretrievably (i.e., previous versions, temporary files and even file fragments are to be deleted as well).

The cloud client should make sure that the cloud provider ensures secure erasure and that the contract between the provider and the client contains clear provision for the erasure of personal data. The same holds true for contracts between cloud providers and subcontractors.

## Contractual safeguards: Controller/Processor relationship

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 organisational measures governing the processing to be carried out, and must ensure compliance with those measures. Furthermore, they are legally obliged to sign a formal contract with the cloud service provider, as stated in the 7th Data Protection Principle. This establishes the requirement for there to be a contract or other binding legal act to govern the relationship between the controller and the processor.

For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the technical and organisational measures shall be in writing or in another equivalent form.

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 organisational measures to adequately protect personal data.

To ensure legal certainty the contract should also set forth the following issues:

1. 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).

2. 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. This is without prejudice to the application of more stringent measures, if any, that may be envisaged under the client's national law.

3. 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.

4. 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.

5. 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 authorised persons can have access to data.

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

7. 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 sub-processors 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. 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 sub-processors, based on the standard contractual clauses.

8. 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.

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

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

11. 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.

12. 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.

13. 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.

14. 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.

In the event of infringement by the controller, any person suffering damages as a result of unlawful processing shall have the right to receive compensation from the controller for the damages caused. Should the processors use the data for any other purpose, or communicate them or use them in a way that breaches the contract, they shall also be considered to be controllers, and shall be held liable for the infringements in which they were personally involved.

It should be noted that, in many cases, cloud service providers offer standard services and contracts to be signed by controllers, which set forth a standard format for processing personal data. This imbalance in the contractual power of a small controller with respect to large service providers should not be considered as justification for the controllers to

accept clauses and terms of contracts which are not in compliance with data protection law.

## International transfers

The 8th Data Protection Principle 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. Otherwise specific safeguards must be put in place by the controller and its co-controllers and/or processors. However, cloud computing is most frequently based on a complete lack of any stable location of data within the cloud provider's network. Data can be in one data centre at 2pm and on the other side of the world at 4pm. The cloud client is therefore rarely in a position to be able to know in real time where the data are located or stored or transferred. In this context, the traditional legal instruments providing a framework to regulate data transfers to non-EU third countries not providing adequate protection, have limitations.

Adequacy findings are limited in respect of the geographical scope, and therefore do not cover all transfers within the Cloud.

In addition, the 7th Data Protection Principle requires a contract to be signed from a controller to a processor for processing purposes. This contract is not subject to prior authorization from the European DPAs. Such contract specifies the processing to be carried out and any measures necessary to ensure that the data are kept secure. Different national legislations and DPAs may have additional requirements.

The exemptions to the 8th Data Protection Principle provided by Schedule 4 of the Law enable data exporters to transfer data out of the EEA without providing additional guarantees. However, WP29 has adopted an opinion in which it considered that exemptions shall apply only where transfers are neither recurrent, nor massive or structural.

Based on such interpretations, it is almost impossible to rely on exemptions in the context of cloud computing.

## Conclusions and recommendations

Businesses and administrations wishing to use cloud computing should conduct, as a first step, a comprehensive and thorough risk analysis. This analysis must address the risks related to processing of data in the cloud by having regard to the type of data processed in the cloud. Special attention should also be paid to assessing the legal risks regarding data protection, which concern mainly security obligations and international

transfers. The processing of sensitive data via cloud computing raises additional concerns. Therefore without prejudice to national laws such processing requires additional safeguards. The conclusions below are meant to provide a checklist for data protection compliance by cloud clients and cloud providers based on the current legal framework.

**Cloud client's responsibility as a controller:**

The client as the controller must accept responsibility for abiding by data protection legislation and is subject to all the legal obligations mentioned in the Law, in particular vis-à-vis data subjects. The client should select a cloud provider that guarantees compliance with the Law as reflected by the appropriate contractual safeguards;

**Subcontracting safeguards:**

Provisions for subcontractors should be provided for in any contract between the cloud provider and cloud clients. The contract should specify that sub-processors 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. The cloud provider should sign a contract with each subcontractor reflecting the stipulations of his contract with the cloud client; the client should ensure that it has contractual recourse possibilities in case of contractual breaches by the provider's sub-contractors;

**Compliance with fundamental data protection principles:**

- Transparency: cloud providers should inform cloud clients about all (data protection) relevant aspects of their services during contract negotiations; in particular, clients should be informed about all subcontractors contributing to the provision of the respective cloud service and all locations in which data may be stored or processed by the cloud provider and/or its subcontractors (notably, if some or all locations are outside of the European Economic Area (EEA); the client should be provided with meaningful information about technical and organisational measures implemented by the provider; the client should as a matter of good practice inform data subjects about the cloud provider and all subcontractors (if any) as well as about

locations in which data may be stored or processed by the cloud provider and/or its subcontractors;

- Purpose specification and limitation: the client should ensure compliance with purpose specification and limitation principles and ensure that no data is processed for further purposes by the provider or any subcontractors. Commitments in this respect should be captured in the appropriate contractual measures (including technical and organisational safeguards);

- Data retention: the client is responsible for ensuring that personal data are erased (by the provider and any subcontractors) from wherever they are stored as soon as they are no longer necessary for the specific purposes; secure erasure mechanisms (destruction, demagnetisation, overwriting) should be provided for contractually.

**Contractual safeguards:**

- In general: the contract with the provider (and the ones to be stipulated between provider and sub-contractors) should afford sufficient guarantees in terms of technical security and organisational measures and should be in writing or in another equivalent form. The contract should detail the client's instructions to the provider including subject and time frame of the service, objective and measurable service levels and the relevant penalties (financial or otherwise); it should specify the security measures to be complied with as a function of the risks of the processing and the nature of the data, in line with the requirements made below and subject to more stringent measures as envisaged under the client's national law; if cloud providers aim at making use of standard contractual terms, they should ensure that these terms comply with data protection requirements; in particular technical and organisational measures that have been implemented by the provider should be specified in the respective terms;

- Access to data: only authorised persons should have access to the data; a confidentiality clause should be included in the contract vis-à-vis the provider and its employees;

- Disclosure of data to third parties: this should be regulated only via the contract, which should include an obligation for the provider to name all its sub-contractors – e.g. in a public digital register – and ensure access to information for the client of any changes in order to enable him to object to those changes or terminate the contract; the contract should also require the provider to notify any legally binding request for disclosure of the personal data by a law enforcement authority, unless such disclosure is otherwise prohibited; the client

should warrant that the provider will reject any non-legally binding requests for disclosure;

- Obligations to co-operate: client should ensure that the provider is obliged to co-operate with regard to the client's right to monitor processing operations, facilitate the exercise of data subjects' rights to access/correct/erase their data, and (where applicable) notify the cloud client of any data breaches affecting client's data;

- Cross-border data transfers: The cloud client should verify if the cloud provider can guarantee lawfulness of cross-border data transfers and limit the transfers to countries chosen by the client, if possible. Transfers of data to non-adequate third countries require specific safeguards via the use of standard contractual clauses (SCC) or binding corporate rules (BCR) as appropriate; the use of SCC for processors requires certain adaptations to the cloud environment (to prevent having separate per-client contracts between a provider and its sub-processors) which might imply the need for prior authorisation from the competent DPA; a list of the locations in which the service may be provided should be included in the contract;

- Logging and auditing of processing: the client should request logging of processing operations performed by the provider and its sub-contractors; the client should be empowered to audit such processing operations, however third-party audits chosen by the controller and certification may also be acceptable providing full transparency is guaranteed (e.g. by providing for the possibility to obtain a copy of a third-party audit certificate or a copy of the audit report verifying certification);

- Technical and organisational measures: these should be aimed at remedying the risks entailed by lack of control and lack of information that feature most prominently in the cloud computing environment. The former include measures aimed at ensuring availability, integrity, confidentiality, isolation, intervenability and portability.

# Contact the Commissioner

## Enquiries and Publication Requests

Jersey

**Office of the Information Commissioner**
Brunel House
Old Street
St Helier
Jersey
JE2 3RG

T: +44 (0)1534 716530
W: www.dataci.org
Email: enquiries@dataci.org

Guernsey

**Office of the Data Protection Commissioner**
Guernsey Information Centre
North Esplanade
St Peter Port
Guernsey
GY1 2LQ

T: +44 (0)1481 742074
W: www.dataci.org
Email: enquiries@dataci.org