The Impact of GDPR on Cloud Service Providers:

Negotiating and Managing Data Processing Agreements

25/06/2019 | Filipe Lousa, Global DPO

The Impact of GDPR on Cloud Service Providers:

Negotiating and Managing Data Processing Agreements

- Cloud computing is the practice of using a network of remote servers hosted on the internet to store, manage, and process data, rather than a local server or a personal computer.
- A cloud service provider (“CSP”) is a company that offers some component of cloud computing – typically:

IaaS
Infrastructure as a Service

PaaS
Platform as a Service

SaaS
Software as a Service

The Impact of GDPR on Cloud Service Providers:

Negotiating and Managing Data Processing Agreements

- **IaaS:** the CSP delivers infrastructure components that would otherwise exist in an on-premises data center. These components could consist of servers, storage and networking as well as the virtualization layer, which the IaaS provider hosts in its own data center. Cloud service providers may also complement their IaaS products with services such as monitoring, security, and storage resiliency.
- **PaaS:** the CSP offers cloud infrastructure and services that users can access to perform various functions. PaaS products are commonly used in software development. In comparison to an IaaS provider, PaaS providers will add more of the application stack, such as operating systems andmiddleware.
- **SaaS:** the CSP offers hosts applications and makes them available to customers over the Internet, such as productivity suites, CRM software and HRM software.

The Impact of GDPR on Cloud Service Providers:

Negotiating and Managing Data Processing Agreements

When the CSP supplies the means and the platform, acting on behalf of the cloud client, the CSP is considered as a data processor under GDPR, art. 28. Therefore, to keep controllership in order to ensure full compliance with GDPR and be accountable, the controller shall:

- Select a CSP providing sufficient guarantees in respect of the technical and non-technical measures it is capable to implement to assist the controller in complying and ensure the data protection rights of the data subjects whose data are processed.
- Enter into a legally binding contract between the CSP and the controller, i.e., a Data Processing Agreement ("DPA").
- Ensure and monitor the implementation of the required safeguards and other contractual provisions.

Contracting: Getting the right Terms & Conditions

The Impact of GDPR on Cloud Service Providers:

Negotiating and Managing Data Processing Agreements

- **Sole controllership**

The CSP shall process the personal data **only on behalf of the controller** and **in compliance with its documented instructions and the DPA**.

Sample:

- *The CSP shall only process Personal Data on behalf of the Controller and in accordance with its documented instructions, including with regard to transfers of Personal Data to a country outside of the European Economic Area, unless required to do so by Union or Member State law to which CSP is subject; in such a case, the CSP shall inform the Controller of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest.*

The Impact of GDPR on Cloud Service Providers:

Negotiating and Managing Data Processing Agreements

- **Processing of Personal Data**

The Supplier will process the Personal Data of the Data Subjects as further described in the DPA and in its Schedules. Pursuant to Article 28(3) and Article 28(9) of the GDPR, the following elements describing the processing shall in any case be set out in the contract, which shall be in writing, including in electronic form:

- the subject matter / the duration of the processing / the nature and purpose of the processing;
- the type of personal data / the categories of data subjects / the obligations and rights of the controller;
- The locations where personal data may be processed / Sub processors engaged
- The appropriate technical and organisational measures / Auditing

The Impact of GDPR on Cloud Service Providers:

Negotiating and Managing Data Processing Agreements

- **Sub Processing**

The CSP shall not authorise any third party sub-contractor to Process Personal Data unless:

- The prior written authorisation of the Controller has been obtained **(specific or general written authorization)**; and
- The CSP's has in place a written agreement with the sub-contractor (or sub-sub-contractor as the case may be) which is on terms substantially the same as those set out in the DPA; and
- The CSP's written agreement with the sub-contractor (or sub-sub-contractor as the case may be) provides that it shall terminate automatically on the termination of the DPA; and
- The CSP shall, at all times, be fully liable to the Controller for the performance by the sub-contractor (or sub-sub-contractor) of its obligations as if the CSP were performing those obligations itself.

The Impact of GDPR on Cloud Service Providers:

Negotiating and Managing Data Processing Agreements

Sample

- ***Current Sub-processor List****. Controller acknowledges and agrees that CSP may engage its current Sub-processors listed at (***Link***).* ***Written Notice Via Mailing List****. CSP will provide Controller with notice ("New Sub-processor Notice") of the addition of any new Sub-processor to the Sub- processor List at any time during the term of the Agreement. CSP will provide Controller with additional information about any Sub-processor on the Sub-processor List that Controller may reasonably request upon receipt of a New Sub-processor Notice*
- ***Controller Objection****. If Controller has a reasonable basis to object to CSP's use of a new Sub-processor, Controller will notify CSP promptly in writing within X days after receipt of a New Sub-processor Notice. CSP will use reasonable efforts to make available to Controller a change in the affected Services or recommend a commercially reasonable change to Controller's configuration or use of the affected Services to avoid processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Controller. If CSP is unable to make available such change within a reasonable period of time, which will not exceed X days, Controller may terminate the portion of any Agreement relating to the Services that cannot be reasonably provided without the objected-to new Sub-processor by providing written notice to CSP.*
- ***Responsibility****. CSP will remain responsible for its compliance with the obligations of this DPA and for any acts and omissions of its Sub-processors that cause CSP to breach any of CSP's obligations under this DPA.*

The Impact of GDPR on Cloud Service Providers:

Negotiating and Managing Data Processing Agreements

- **Security Measures**

The CSP shall implement appropriate technical and organizational security measures sufficient to guarantee that its Processing of the Personal Data meets the requirements of the Data Protection Legislation and ensures the protection of the rights of the Data Subjects.

In addition the CSP shall ensure that it has in place appropriate technical and organisational measures to protect against the unauthorised or unlawful Processing of the Personal Data and against accidental loss, or destruction, or damage, to Personal Data appropriate to the harm that might result from such unauthorised or unlawful Processing or accidental loss, destruction or damages and the nature of the Personal Data to be protected, having regard to the state of technological development and the cost of implementing such measures

The Impact of GDPR on Cloud Service Providers:

Negotiating and Managing Data Processing Agreements

Those measures may include as appropriate:

- the pseudonymisation and encryption of Personal Data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of the Data Processing System and Services;
- the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident - SLAs;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing;
- appropriate (preventive) measures that enable CSP to immediately detect a Data Breach and inform the Controller.

The Impact of GDPR on Cloud Service Providers:

Negotiating and Managing Data Processing Agreements

Sample:

- ***Security***. *CSP will keep Controller's Data confidential and implement and maintain administrative, physical, technical and organizational safeguards for the security (including protection against accidental or unlawful loss, destruction, alteration, damage, unauthorized disclosure of, or access to, Controller Data transmitted, stored or otherwise Processed), confidentiality and integrity of Controller Data as detailed in Annex X*

The Impact of GDPR on Cloud Service Providers:

Negotiating and Managing Data Processing Agreements

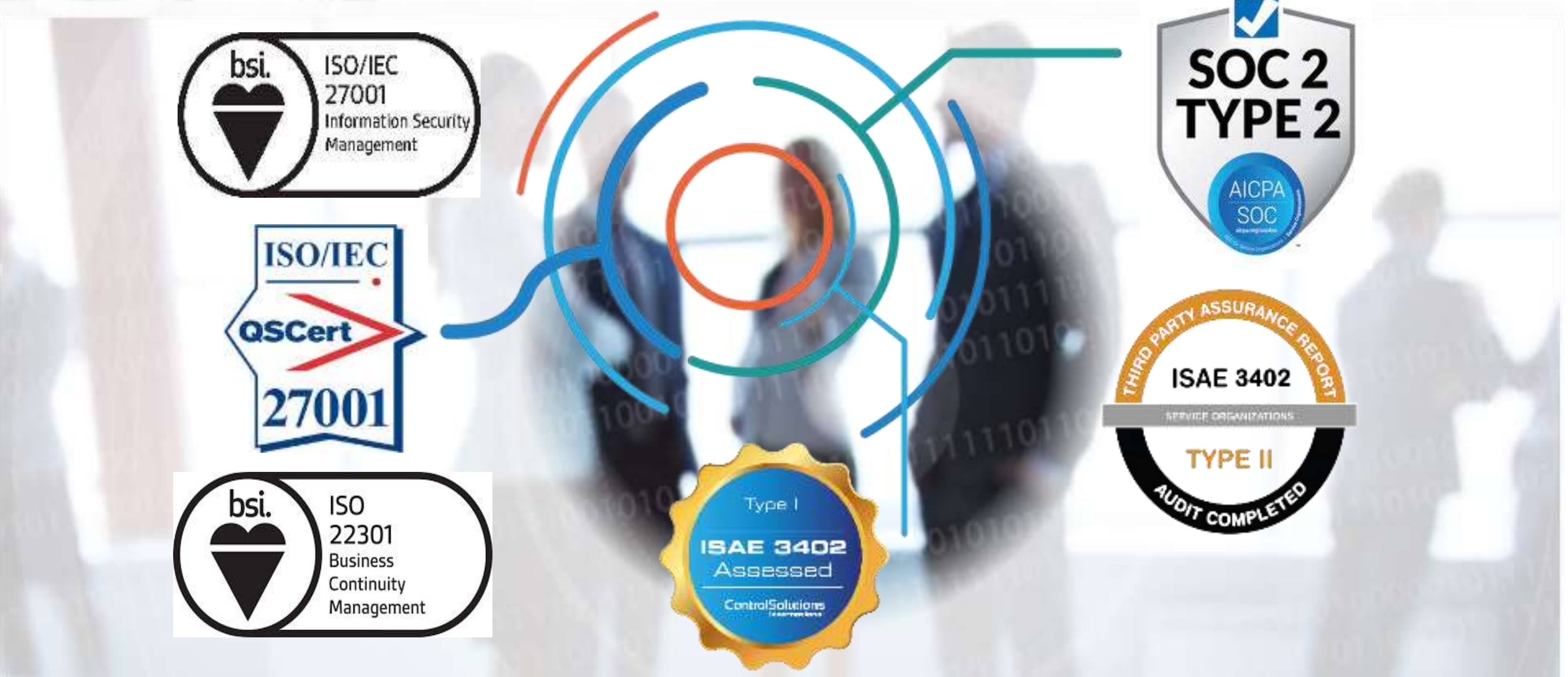
- **Third Party Certifications and Audits**

In addition to its specific information and reporting obligations under the DPA and the Data Protection Legislation, the CSP shall make available to Controller all information reasonably necessary to demonstrate compliance with the DPA and the Data Protection Legislation, and allow for and contribute to audits, including inspections, conducted by Controller, or an auditor mandated by Controller

Why You should trust Getronics?

Getronics applies security best practices and manages security to allow Customers to focus primarily on their business.

Getronics


bsi. ISO/IEC 27001 Information Security Management
ISO/IEC QSCert 27001
bsi. ISO 22301 Business Continuity Management
Type I ISAE 3402 Assessed ControlSolutions
SOC 2 TYPE 2
AICPA SOC
THIRD PARTY ASSURANCE REPORT
ISAE 3402
SERVICE ORGANIZATIONS
TYPE II
AUDIT COMPLETED

The Impact of GDPR on Cloud Service Providers:

Negotiating and Managing Data Processing Agreements

Sample:

- ***Certification/Security Reports****. In addition to the information contained in this DPA, upon Controller's request, and subject to the confidentiality obligations set forth in the Agreement place, CSP will make available the following documents and information regarding the System and Organization Controls (SOC) 2 Report (or the reports or other documentation describing the controls implemented by CSP that replace or are substantially equivalent to the SOC 2), so that Controller can reasonably verify CSP's compliance with its obligations under this DPA.*
- ***Audits****. To the extent the reports provided in Section above do not verify CSP's compliance with its obligations under this DPA, Controller may audit CSP's compliance with this DPA up to once per year, unless requested by a Supervisory Authority or in the event of a Security Incident. (…)*

The Impact of GDPR on Cloud Service Providers:

Negotiating and Managing Data Processing Agreements

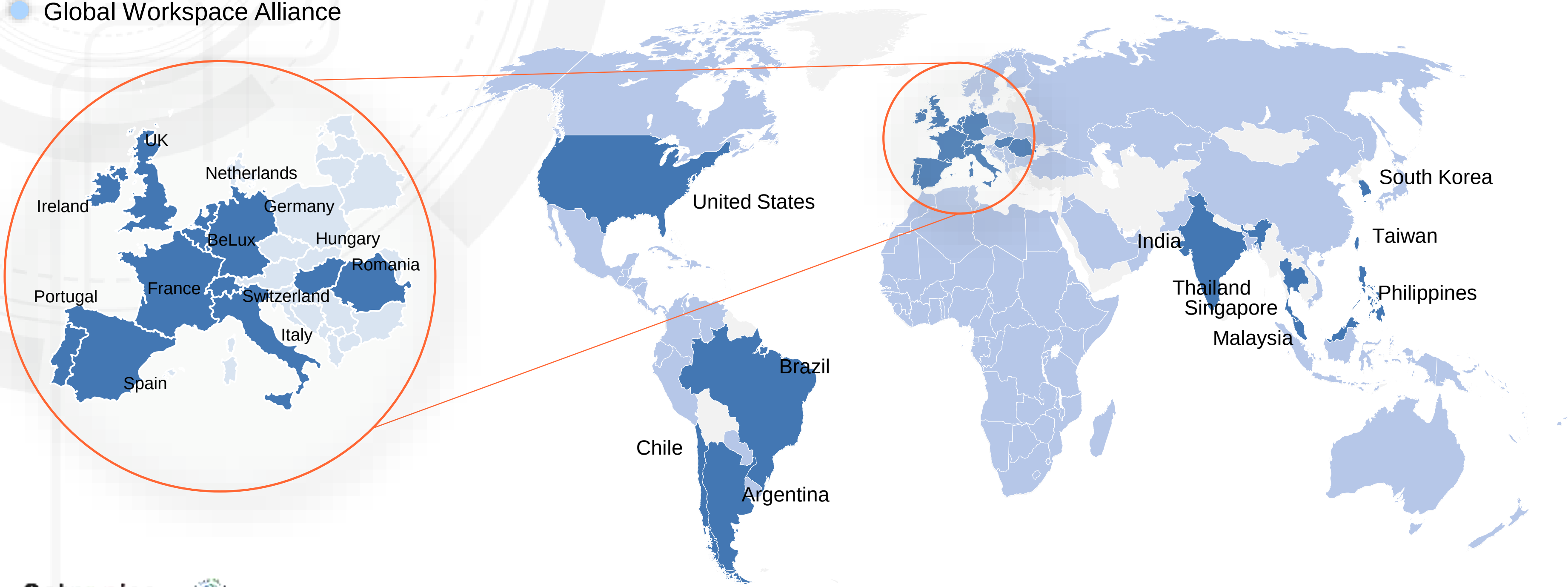
- **Transfers of Personal Data**

The CSP shall not transfer any Personal Data outside the European Economic Area (EEA) without Controller prior written consent.

Global Coverage with Local Strength

UNIQUE GLOBAL APPROACH

- ● The Getronics Group
- ● Global Workspace Alliance



The Impact of GDPR on Cloud Service Providers:

Negotiating and Managing Data Processing Agreements

The provision of Controller written consent shall be granted only on the following conditions:

- the CSP shall ensure that any transfer or Processing of Personal Data outside the EEA is carried out in accordance with the requirements of the Data Protection Legislation; and
- One of the following conditions is met:

a) The CSPs and/or any third party it engages is Processing Personal Data in a territory which is subject to a current finding by the European Commission under the Data Protection Legislation that the territory provides adequate protection for the privacy rights of individuals (adequacy decision).

The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the United States of America (limited to the Privacy Shield framework) as providing adequate protection.

The Impact of GDPR on Cloud Service Providers:

Negotiating and Managing Data Processing Agreements

b) The CSP participates in a valid cross-border transfer mechanism under the Data Protection Legislation, so that the CSP (and, where appropriate, Controller) can ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals as required by Article 46 of GDPR.

Example:

- Binding corporate rules in accordance with Article 47;

- EU Standard Contractual Clauses

The Impact of GDPR on Cloud Service Providers:

Negotiating and Managing Data Processing Agreements

Sample

- *To the extent Services involve a transfer of Personal Data originating from the European Economic Area ("EEA") or Switzerland to CSP Affiliates or Third Party Subprocessors located in countries outside the EEA or Switzerland that have not received a binding adequacy decision by the European Commission or by a competent national EEA Supervisory Authority, such transfers are subject to the terms of the Standard Contratual Clauses incorporated into this Data Processing Agreement by reference which includes **Appendix 1** (Details of the Transfer) and **Appendix 2** (Technical and Organizational Measures), both as attached hereto in Schedule X. For the purposes of the Standard Contractual Clauses, the Controller and CSP agree that (i) the Controller will act as the data exporter, (ii) CSP will act on its own behalf and/or on behalf of the relevant CSP Affiliates as the data importers, (iii) any Third Party Subprocessors will act as 'subcontractors' pursuant to Clause 11 of the Standard Contractual Clauses*

The Impact of GDPR on Cloud Service Providers:

Negotiating and Managing Data Processing Agreements

- **Reporting of Data Breaches**
- The CSP shall maintain adequate procedures designed to detect and respond to all Data Breaches, including procedures for preventive and corrective actions, and also to avoid recurrence of any Data Breach so as to enable Controller or the Controller (where this is not Controller) to meet its Data Breach reporting obligations under the Data Protection Legislation.
- As soon as the CSP detects a Data Breach or reasonably suspects that a Data Breach has occurred or could occur, it shall notify Controller without undue delay.
- The CSP shall also co-operate fully with Controller to enable Controller to fully comply with its obligations in respect of the notification of the Data Breach to the relevant Supervisory Authority, the communication of the Data Breach to the affected Data Subject(s) and the recording of Data Breaches internally

The Impact of GDPR on Cloud Service Providers:

Negotiating and Managing Data Processing Agreements

- **Requests of Data Subjects**

The CSP shall provide full assistance to Controller in responding to any request from a Data Subject and in ensuring compliance with Controller obligations under the Data Protection Legislation with respect to security, breach notifications, impact assessments and consultations with Supervisory Authorities.

Sample:

- ***Data Subject Requests.*** *If CSP receives a request from any Data Subject made under Data Protection relating to Controller Data, CSP will provide a copy of that request to the Controller within two (2) business days of receipt. CSP provides Controller with tools to enable Controller to respond to a Data Subjects' requests to exercise their rights under the Data Protection Laws.*

The Impact of GDPR on Cloud Service Providers:

Negotiating and Managing Data Processing Agreements

- ***Applicable law and Jurisdiction***

The DPA shall be governed by EU law and, where applicable in accordance with EU law, by the law of the EU Country where the controller is established or any other applicable law of an EU Country.

Sample

- ***GOVERNING LAW AND JURISDICTION.*** *Except where the Processing of the Personal Data is governed by specific Data Protection Laws, in such case such laws shall apply, this DPA shall be governed by, and construed and enforced in accordance with the laws defined in the Master Services Agreement, excluding its rules regarding the conflict of laws.*

- **Requests of Supervisory Authority**

The CSP shall assist Controller in addressing any communications and abiding by any advice or orders from the Supervisory Authority relating to the Personal Data

Ensuring Control

Obligations after the Termination

The Impact of GDPR on Cloud Service Providers:

Negotiating and Managing Data Processing Agreements

On the termination of the provision of data **processing services**, the CSP and the sub-processors shall, at the choice of the controller:

- without any delay, in a commonly agreed format, either **return all the personal data and the copies thereof to the controller** or **transfer them to a destination designated** by the controller itself.

  The CSP shall ensure and be able to demonstrate the '**portability' of the controller's data from its systems, and any sub-processor system, to other providers** of the controller's choice, within the time frame and in the format specified in the DPA.

  The CSP must ensure that the controller is provided fully with the service and access to the data during this period.

  The CSP and any sub-processor shall keep the controller's data safe and secure until transferred to another site as instructed by the controller.

The Impact of GDPR on Cloud Service Providers:

Negotiating and Managing Data Processing Agreements

- or **delete all the personal data and certify to the controller that it has done so.**

Sample:

On termination of the processing services, the CSP shall be under obligation, at the Controller’s discretion, to erase or return, in a common agreed format and free of charge, all the Personal Data to the Controller and to erase existing copies unless EU law or Member State law requires storage of the personal data.

The Impact of GDPR on Cloud Service Providers:

Negotiating and Managing Data Processing Agreements

THANK YOU!

Filipe Lousa

filipe.lousa@getronics.com