28 November 2017

CISPE Response to the public consultation on the Article 29 Data Protection Working Party draft "Guidelines on Personal data breach notification under Regulation 2016/679"

Introduction

CISPE welcomes the opportunity to provide comments to the draft data breach notification guidelines published by the Article 29 Data Protection Working Party (the "**WP29**") in relation to the interpretation of the General Data Protection Regulation (the "**GDPR**") (the "**Guidelines**").

CISPE is the voice of Cloud Infrastructure Service Providers in Europe. Our membership currently includes companies operating in 15 European countries. For more information please see https://cispe.cloud.

Specificity of Cloud Infrastructure Services Providers

From the perspective of cloud infrastructure services providers ('**CISPs**'), the Guidelines should take into account the contractual requirements that are specific to the provision of storage and computing infrastructure to customers, without access to the data stored or processed by such customers or data controllers.

CISPs enable their customers to achieve a very high degree of technical and financial flexibility. Sometimes, they are suppliers on which other Cloud computing actors build their own services for their customers ('Cascade of cloud suppliers') practically involving several sub-processors and/or co-controllers.

Without a system of notifications – from the controller to their processor, and vice versa when applicable - there could be insufficient information for deciding which type of incidents have to be notified, how such incidents should be addressed and if they constitute a data breach; and what information needs to be made available following a specific incident, even if it does not involve a data breach.

With the above in mind, CISPE's response focuses on areas where we believe improvements can be made with regard to the practical implementation mainly on page 11 of the Guidelines[1].

1. Imputing the processor's awareness to the controller

By imputing the processor's awareness to the controller, irrespective of whether the processor (the CISP) has already notified the controller, or if the controller has provided the processor (the CISP) with the required information under the applicable service agreement security incident management policies, it makes the data breach notification requirement technically difficult, if not impossible, to implement in practice.

[1] *"The controller uses the processor to achieve its purposes; therefore, in principle, the controller should be considered as "aware" once the processor has become aware. (…) Therefore, WP29 recommends an immediate notification by the processor to the controller, with further information about the breach provided in phases as information becomes available."*

Cloud Infrastructure Service Providers in Europe ASBL www.cispe.cloud
32 Ernest Solvay, Bruxelles, B-1050 Belgium
+32 (0)2 513 55 09 - info@europa-insights.com
EU Transparency Register: 041495920038-44

The nature of cloud infrastructure services is such, that certain technical aspects of data security – including in relation to potential data breaches - are the customer's sole responsibility and that the knowledge of these technical aspects by the CISP impacts on its ability to fulfil its legal obligations (as processor). For example, the customer (and not the CISP) will be responsible for the security of guest operating systems, applications hosted on the service, data in transit and at rest, customer's service log-in credentials and permissions policies for customer personnel using the service.

Conversely, if the CISP becomes aware of unauthorised access to any customer personal data on the CISP's equipment or in the CISP's facilities and such unauthorised access results in loss, disclosure or alteration of that data, the CISP will notify the customer without undue delay based on a typical service agreement.

All CISP service agreements must implement security incident management policies that specify the procedures for identifying, and responding to security incidents, including for potential data breaches, of which either the CISP (processor) or their customers (controller) become aware. Similarly, under most service agreements security incident management policies, cloud infrastructure customers must, for example, notify the processor of any incidents without undue delay - ranging from 24 to 72 hours - depending on the type of security incidents.

For these reasons, we caution against imputing the processor's awareness to the controller, irrespective of whether the processor has already notified the controller and strongly recommend that the Guidelines follows the two-stage process as defined in Article 33 of the GDPR.

2. When to notify the controller

If the CISP becomes aware of unauthorised access to any customer personal data on the CISP's equipment or in the CISP's facilities and such unauthorised access results in loss, disclosure or alteration of that data, the CISP will notify the customer without undue delay (see Article 33(2) of the GDPR).

With respect to processors, however, the Guidelines recommend an "immediate" notification.

We believe that the same logic as we described in point 1, should apply here, i.e. that processors, just like controllers, should be enabled to investigate potential data breaches before they notify them further.

Taking away the time to properly investigate the parameters of potential data breaches, could lead to notifications that are incorrect and thus too early or unnecessary. These could create unjustified concerns and undermine public trust in the digital economy.

We suggest here that the Guidelines follow the obligation as defined in Article 33(2) of the GDPR.

3. Types of personal data breach

The Guidelines refer to "*availability breach*" as one of the categories of relevant breaches and state that "*an incident resulting in personal data being made unavailable for a period of time is a security breach (and should be documented)*" (page 7 of the Guidelines).

Treating unavailability as a security issue brings availability breaches under the definition of "*personal data breach*" in the GDPR. However, merely temporary losses of availability of personal data should not be considered a breach by that measure alone, particular when such occurrences are contemplated in service agreements, for example for voluntary maintenance purposes or any other contractually agreed or permitted instances of unavailability.

According to the Guidelines, all such temporary losses of availability are recordable events and, depending on whether it is likely to result in a risk to the rights and freedoms of natural persons, may also be reportable. From a practical point of view, it is difficult to record all such temporary losses of availability, particularly without having access to the data that will be stored or processed by our customers, or data controllers.

We would welcome clarification that temporary losses of availability are not necessarily "*personal data breaches*" particular when such occurrences are merely temporary and contemplated in the applicable service agreements.

CISPE is happy to constructively engage with WP29 in the implementation of this crucial piece of EU privacy legislation. We trust that CISPE recommendations will be taken into consideration and remain at your disposal should you wish to discuss the matter in more technical details.

***