Awareness raising campaign for SMEs

Guidance for Organisations Engaging Cloud Service Providers

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S RIGHTS, EQUALITY AND CITIZENSHIP 2014-2019 PROGRAMME UNDER GRANT AGREEMENT N°874524.

Contents

One of the main obligations under the General Data Protection Regulation (GDPR) for organisations which process personal data ('controllers'), is that they must do so in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing (including theft, destruction or damage, or disclosure) using 'appropriate technical or organisational measures'. This is sometimes referred to as the principle of 'integrity and confidentiality' or the 'security principle'.

This obligation is an important one, which controllers should be cognisant of, particularly those who utilise or store sensitive personal data. Whether or not an organisation has appropriate technical and organisational measures in place to ensure the security of the personal data they process is one of the first questions the Data Protection Commission (DPC) is likely to ask in the event of a personal data breach or the exercise of the DPC's investigative powers. Controllers can also consult our guidance for controllers on data security when assessing the appropriate security measures they need to implement.

There are an increasing number of services offering 'cloud storage', allowing documents, photos, videos, and other files be uploaded to and stored on a remote server, to enable sharing or remote access, or to act as a backup copy. The use of any cloud services as part of their business is an important area in which organisations need to ensure there is adequate security for the personal data they process.

A risk to the security of personal data can arise where a data controller relinquishes control over the data to a cloud service provider, where there is insufficient information available regarding the cloud processing services and their safeguards, or where the cloud provider cannot adequately support the data controller's obligations or data subjects' rights.

A data controller must remain in control of the personal data it collects when it subcontracts the processing to a cloud provider. A key element of control is to ensure the security of the data. Controllers (both clients and cloud service providers) also need to be transparent about the processing of personal data. Important for both control and security is the location of the data. A related issue is also the requirement for a written contract.

What is 'cloud computing'?

People often mean different things when they talk of processing data 'in the cloud'. For an organisation processing personal data, it usually involves using an external cloud service provider doing some or all of the processing or storage on servers and/or in a data centre under that provider's control. In many cases, external service providers will be acting as data 'processors', which also have a number of responsibilities under the GDPR, although less than those which apply to controllers. A processor is any person or organisation which processes personal data on behalf of and on the instructions of the controller.

There are generally three different service models for cloud computing available to organisations. In its most advanced form, the cloud provider takes care of all aspects of the processing of the data on behalf of the client, apart from the raw data inputted by individual users. The cloud organisation thus provides:

- ☑ the physical infrastructure in a datacentre;
- ☑ the operating system to run the necessary software; and
- ☑ the software needed to process the data itself.

This is sometimes referred to as 'Software as a Service' or 'SaaS'.

A client (the data controller) may also choose to avail of only part of the service available from a cloud provider – for example, server space only (sometimes referred to as 'Infrastructure as a Service' or 'IaaS') or server space plus software tools (sometimes referred to as 'Platform as a Service' or 'PaaS').

A further distinction often made is between a 'private cloud' – where the cloud provider dedicates resources to a specific client – and a 'public cloud' – where the client may operate in a multi-tenanted environment involving shared systems and infrastructure. There can also be 'hybrid' versions of the above where there is a mixture of processing and data sharing between the data controller's own infrastructure and the cloud provider's infrastructure.

Cloud providers generally provide processing services to data controllers but may also provide sub-processing services to other providers. In some cases however, cloud providers are also data controllers, or 'joint controllers'. In such cases, they are subject to more onerous obligations under GDPR than when acting as a processor. This guidance primarily addresses cloud providers acting as processors, and the controllers who engage with them.

What are the security considerations around cloud computing?

Article 28(1) GDPR necessitates that only processors providing sufficient guarantees to implement appropriate technical and organisational measures may be engaged by a controller. Furthermore, Article 32 GDPR requires that the controller and processor implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. An approved code of conduct (Article 40 GDPR) or approved certification mechanism (Article 42 GDPR) can be used to supplement compliance with Article 32 GDPR. A controller must therefore be satisfied that personal data will be secure if it is outsourced to a cloud provider.

Security in this context has two main aspects:

- First, the controller must be satisfied that the processor (the cloud provider) will only process the data in accordance with the controller's instructions. This is directly related to the need for a contract between controller and cloud provider.
- Second, the controller must be satisfied that the cloud provider has taken into account the risks presented from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

A controller, before considering entrusting personal data to a cloud provider, must be satisfied that the cloud provider's security standards are sufficient and appropriate for the processing of personal data they will undertake on the controller's behalf. The cloud provider should be in a position to give assurances on key issues such as:

- ☑ The pseudonymisation and encryption of personal data if required.
- ☑ The isolation or separation of a personal data provided by the controller from the cloud provider's other customers' data.
- ☑ The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services. This encompasses the organisational and technical means, from staff confidentiality requirements to meeting the security requirements of Article 32 GDPR.
- ☑ The ability to restore availability and access to personal data in a timely manner in the event of a physical or technical incident.
- ☑ A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
- ☑ Procedures in the event of a data breach. This will practically mean that an incident response plan is in place and that a binding agreement on breach notification between the processor and controller is made, so that data subjects are not unnecessarily put at risk.
- ☑ A means to delete or return all personal data to the controller when a contract terminates.

A cloud client must seek to assure themselves on the above matters, both in advance of retaining a particular cloud provider and throughout any contractual arrangement entered into. This would typically be achieved by way of a detailed technical analysis incorporating an information security audit questionnaire of the cloud provider and/or any approved code of conduct or certification mechanism provided by the cloud provider as assurance. In some cases it may also necessitate on-site inspection of premises, the way the organisation has implemented their security policy, or audit of particular personal data processing operations or technology usage.

What are the transparency requirements?

In order for a controller to understand how a cloud provider can service their processing needs in a GDPR-compliant manner, a high level of transparency is required. This means that the cloud provider must be able to account for its processing operations to the satisfaction of its customers. Controllers should also provide transparent information to data subjects that the processing of their personal data is undertaken with the use of cloud processing services.

Transparency is therefore an important element in the decision making of individuals when availing of controller's services.

As noted above, an audit questionnaire may be sufficient in some cases to meet cloud providers obligations under Article 28(3)(h) GDPR, allowing controllers to perform audits of their operations. A key part of this audit will focus on the security arrangements. Note that, as cloud providers will typically provide services to multiple data controllers and have security and confidentiality obligations with each, the extent and detail of what is made available in that audit may be restricted.

Article 30(2) GDPR on record keeping also applies in the case of cloud providers. As part of the accountability requirements of GDPR, this means that a processor should document and be able to make available to a controller the basic information specified.

Under Article 28(2) and 28(4) GDPR cloud providers, as processors, also need to provide their controllers with information regarding any sub-processors they engage to provide their services. This means that a controller can review this arrangement under contract terms and allows the controller to object to sub-processing if needed.

Article 28(5) GDPR sets out that a cloud provider as a processor can also avail of approved codes of conduct or approved certification mechanisms to help demonstrate the compliance of elements of their processing. It is important that the nature, scope and context of such codes or certification is clear to controllers so that they can adequately understand to what extent it applies to the processing of their personal data, and if it is appropriate to the processing operations that are being contracted.

Does it matter where the data is located?

Personal data that is held within the European Economic Area (EEA)(EU Member States plus Iceland, Liechtenstein, and Norway) benefits from a common standard of protection laid down at EU level. When data is transferred outside of the EEA, special measures must be taken to ensure that it continues to benefit from adequate protection. The range of options is set out in the DPC's guidance on international transfers. In practice, where a cloud provider is processing personal data outside of the EEA, one of the following mechanisms must be relied upon:

- ☐ The data transfer takes place based on an adequacy decision,[1] as specified in Article 45 GDPR
- ☐ The data transfer is subject to appropriate safeguards (such as EU approved model contracts) as specified in Article 46 GDPR
- ☐ The data transfer is subject to binding corporate rules in accordance with Article 47 GDPR

[1] See European Commission, Adequacy Decisions, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

Where 'model contracts' or 'binding corporate rules' are used, it is important that the protections afforded by these mechanisms also extend to any sub-processors engaged by the cloud provider.

What kind of contract does use of a cloud service require?

Article 28(3) GDPR requires that processing by a processor is governed by a contract. Furthermore, as noted above, a processor is not to engage another processor without the authorisation of the controller. This means that a controller engaging a cloud provider as a processor retains control over the personal data they are processing, that there are agreed and clear limits to that processing, that the processor is clear on their obligations to the controller and that any limits to responsibility and liability for infringements or breach at the processor (cloud provider) is defined.

The contract should include the key points outlined below:

- ☑ That the cloud provider – and any sub-processors used by the provider - will only process the data as instructed by the data controller.
- ☑ Detailed assurance by the cloud provider on security measures and how requirements under Article 32 GDPR will be met.
- ☑ Enumeration of the sub-processors that are engaged by the processor and details on how updates to these are treated with the controller.
- ☑ The information necessary to demonstrate the cloud provider's compliance with Article 28 GDPR and how the processor will allow or contribute to the data controller's audits or inspections.
- ☑ The measures that are provided to guarantee the security of personal data that is processed outside of the European Economic Area.
- ☑ The liability apportioned between the controller and processor in the event of a GDPR infringement or personal data breach, and how such events are notified to the controller.
- ☑ How the processor is meeting their obligations to support a data subject rights.
- ☑ The subject-matter, scope, nature, context, purpose and duration of the processing and how types and categories of personal data are dealt with at commencement, transfer, routine processing and 'end-of-life' – including return or deletion.

More information on how to draft such a contract can be found in the DPC's practical guide to data processor contracts, available on the DPC website.

Further Guidance

The European Network and Information Security Agency (ENISA) has provided helpful guidance, written from a European perspective, on topics including 'Towards secure convergence of Cloud and IoT', 'Technical Guidelines for the implementation of minimum security measures for Digital Service Providers', and 'Cloud Security Guide for SMEs'.

The European Data Protection Supervisor (EDPS), which has responsibility for data protection in the EU institutions, has published 'Guidelines on the use of cloud computing Services by the

European institutions and bodies' which (although based on a slightly different set of laws) may be of practical use to organisations looking to better understand cloud security.

Organisations are reminded that under the GDPR organisations must report personal data breaches to the relevant supervisory authority where the breach presents a risk to the affected individuals. Organisations must do this within 72 hours of becoming aware of the breach. Where a breach is likely to result in a high risk to the affected individuals, organisations must also inform those individuals without undue delay. Further guidance on breach notifications can be found on the DPC's website.