simplisys
SERVICE DESK

GDPR – Data Processors Responsibilities.

Introduction

The Fifth paper in the series looking at the impact of the new GDPR (General Data Protection Regulations) coming in to force on 25th May 2018. This paper looks at the responsibilities of the Data Processors should support Data Controllers and the key aspects to Data Processor selection when processing personal data.

How the Data Processor Supports the Data Controller

We have seen how the GDPR imposes responsibilities on data controllers to ensure the security and integrity of personal data and to support the rights of Data Subjects, but what about Data Processors? What does GDPR have to say about them?

The common belief is that data processors have a rather limited liability for the data under their control, after all it's the responsibility of the data controller to ensure compliance with GDPR. However, nothing could be further from the truth.

In fact Data Processors have most of the same responsibilities as data controllers as well as some specific ones of their own. So if you are a data controller looking to outsource the processing of personal data or use a SaaS platform to process personal data you need to understand how the data processors, the providers of the SaaS platform, responsibilities interact with your own!

Data Processors Responsibilities

Article 28 of the GDPR spells out the responsibilities of the data processor with the very first clause imposing almost all of the same obligations as apply to data controllers!

> *"1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that*

> *processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject."*

The key requirements referred to here are those defined by:

Article 30 which requires that Records of processing be kept,

Article 32 which requires that processing of personal data be done in a secure manner "*processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk,"*

And

Articles 33 and 34 which require breaches of personal data security or integrity to be reported both to the Supervisory authority, the information commissioner's office in the UK, and the data subject(s) who's data has been impacted by the breach.

So as a data processor you are responsible for implementing the required security measures to ensure that the processing meets the requirements of the GDPR. The complexity for data processors, particularly those supplying SaaS products is that no two users of their platform will have the same requirements.

Article 32 requires that *"the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons"* be considered when assessing the security measures to implement. The "*nature, scope, context and purposes"* will quite naturally be different for every user of the SaaS platform so Data Processors need to demonstrate they understand the nature, scope and purposes of the processing being carried out by them on behalf of the data controller and that the technical and organisational measures in place are appropriate to the risk.

In this case one size most definitely does not fit all!

Additional Responsibilities

Article 28 goes on to impose additional responsibilities on a data processor. Clauses 2 and 3 detail the relationship between the data controller and data processor. Specifically, it imposes an obligation on the data processor to only undertake processing in accordance with and with the agreement of the data controller.

One implication of this is that the data processor can only process data in accordance with the data controller's wishes and instructions. A data processor should not, for example, introduce, and activate, a new piece of processing functionality into the SaaS platform without the data controller's agreement. This may be a new application function, which should not be automatically activated, or even a maintenance function such as implementing a 'new' or changed process for archiving old records.

This agreement needs to be in the form of a contract that imposes the obligations discussed above on the Data Processor but additionally the contract should also require the data processor to make any and all information required by the data controller available to him that he might need to demonstrate his compliance with the GDPR. The data processor must be able to furnish the data controller with details of how he has implemented the technical and management measures commensurate with the need to protect the data controller's data and details of all the processing that the controller's data has undergone.

The data processor must also be able to delete the data controller's data or return it to him as requested and delete all existing data as required.

Finally, the Data Processor must not sub contract any data processing to another data processor without the agreement of the data controller and without the same obligations being imposed, by contract, on the new data processor.

Choosing your Data Processor

The onus is on the data controller to ensure that any data processors he works with are able to fulfil their obligations under the GDPR and he should be asking questions of the data processor regarding how they can assure him that they as data processors will support him in complying with the GDPR obligations. Obviously, this could be a major undertaking and the GDPR offers some assistance to the Data Controller in section 5 of article 28 where it says

> *"Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article. "*

External accreditation of would be Data Processors, such as cyber essentials or ISO27001 can be used as evidence that the data processor does meet the requirements of GDPR and will be able to successfully work with the Data Controller to ensure that his data is processes in accordance with the regulation.

Conclusion

The key for data processors is to understand the nature of the data controller's business and data processing needs and not simply apply a one size fits all solution. The data processor will need to work with the controller to ensure that 'appropriate' controls and processes are in place and that lines of communication are established between them.

The data processor also needs to ensure that he understands the requirements and limits of the processing that has, or will be, authorised by the data controller and that all of these agreements and understandings are underpinned by written contracts and agreements.

In out next paper we will be providing a handy toolkit that will help you identify whether or not you, as a data controller or data processor, meets the requirements and obligations set out in the GDPR.

References

The full text of the GDPR

Additional Resources

CYBER ESSENTIALS

ISO 9001
Registered Firm
Certificate No. [illegible]

International
Accreditation Board
Registration No. [illegible]

ISO 9001
Registered Firm
Certificate No. GB2004195

International
Accreditation Board
Registration No. 0044/1

Tel: 01275 240500
Fax: 01275 240501
sales@simplisys.co.uk