Data Processing Agreements: are they really needed under the GDPR?

March 21, 2021

You may have had a customer approach your organization to enter into a data processing agreement and wonder if it is mandatory to do businesses within the scope of the GDPR or if a simple clause that states "*The Service Provider agrees to comply with applicable data protection and privacy laws*" is sufficient to comply with the General Data Protection Regulation (EU 2016/679) ("**GDPR**"). The GDPR requires that a data controller who engages a data processor must enter into a **written contract** or legal act along the lines set out in Article 28.3 of the GDPR.

The **data processing agreement** as it is commonly called is a key contractual document that sets out the responsibilities and liabilities of both controller and processor. If a processor uses another organization (ie a sub-processor or "other" processor) to assist in its data processing of personal data on behalf of a data controller, it needs to have a written contract in place with that sub-processor.

WHAT SHOULD BE INCLUDED IN A DATA PROCESSING AGREEMENT?

In order for an organization to meet the requirements of the GDPR, as a data controller who engages the services of a data processor to process personal data on its behalf, it must enter into a data processing agreement (a written contract or other legal act) which is legally binding on the data processor. Article 28.3 of the GDPR sets out what needs to be included in that written contract:

1. the processor must only act on the controller's

documented instructions unless required by law to act without such instructions;
2. the processor must ensure that its personnel processing the data are subject to a duty of confidence;
3. the processor must take appropriate measures to ensure the security of processing;
4. the processor must only engage sub-processors with the controller's prior authorization and under a written contract (some controllers provides a general authorization to the processor in the data processing agreement);
5. the processor must take appropriate measures to assist the controller to respond to requests from individuals to exercise their rights.
6. taking into account the nature of processing and the information available, the processor must assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
7. the processor must delete or return all personal data to the controller (at the controller's choice) at the end of the services contract or data processing agreement, and the processor must also delete existing personal data unless the law requires its storage; and
8. the processor must submit to audits and inspections.
9. the processor must also give the controller whatever information it needs to ensure that both controller and processor are meeting their obligations under Article 28 of the GDPR.

The below details are also required in a data processing agreement and is usually set out in an Appendix for ease of reference:

1. the subject matter of the processing (*does processing include for example erasure, recording, matching*

conservation of personal data which are required for the service provider to perform the services under the services contract with the controller);
2. the duration of the processing (*usually this is linked to the duration of the services contract with the supplier, but it may be for a shorter period of time*);
3. the nature and purpose of the processing (*will personal data be processed for a specific purpose and will it be processed via a system or manually*?);
4. the type of personal data involved (*does it include special categories of data or confidential information of the controller?*); and
5. the categories of the data subject (*does the personal data belong to an employee or customer of the controller?*)

IS THERE A SPECIFIC FORMAT FOR A DATA PROCESSING AGREEMENT?

There is no specific format and controllers usually propose their form of data processing agreement when engaging a processor. The essential requirement is that the substance of the data processing agreement meets the legal requirements of the GDPR and then the contracting parties are free to determine the form or layout and any additional clauses that they may wish to include (e.g data protection indemnities, contacts of data protection officers of either party and procedures for dealing with a personal data breach involving the personal data being the subject of the data processing agreement).

DATA PROCESSING AGREEMENTS IN PRACTICE

Data Processing Agreements vary in complexity depending on the subject matter of the services contract and in practice can take a considerable amount of time for negotiation depending on the relative bargaining strength of the parties to the contract and the financial value of the transaction. Some controllers opt to include the data processing agreement as a

part of the services contract while others include it as an Appendix to the services contract. Some examples of data processors include commercial agents such as sale agents OR marketing agents and certain consultancy service providers depending on which party determines the “how” and “why” personal data is processed (ie the data controller) and who acts on those instructions (the data processor).

CLOUD SERVICE PROVIDERS AND DATA PROCESSING AGREEMENTS

Cloud service providers (“CSPs”) now have significant responsibilities as data processors and must act solely on the instructions of the data controller when processing personal data. Currently, most CSPs offer their own standard data processing agreements alongside the Software as a Subscription (SaaS) agreement and these may be non-negotiable by a controller wishing to subscribe to use or access the platform being offered by the CSP (e.g a data controller who wishes to use a customer relationship management to efficiently receive and track its customer requests or complaints).

Many CSPs reserve their right to use personal data for various purposes which have not been agreed with their controller (customer) and this is especially common where cloud services are provided at no cost by the CSP. Controllers are required to engage data processors who provide sufficient guarantees such personal data will be processed in accordance with the GDPR. Organizations must, therefore, consider whether the use of CSPs will lead to additional complications and risks and, potentially, to infringement of the GDPR.

Author: Mahmoud Abuwasel
Title: Partner – Disputes
Email: mabuwasel@waselandwasel.com
Profile:
https://waselandwasel.com/about/mahmoud-abuwasel/