Data protection contracts — what tends to be missing and what to do about it

Drawing on recent guidance from regulators, Rocio de la Cruz, Principal Associate with Gowling WLG, advises on how to legitimise controller-to - processor and joint controller contracts

The GDPR has required organisations to adapt from relying on vague and generic data protection clauses that were in many cases included by default in services agreements to the stringent requirements of Article 28 regarding controller-processor arrangements. Organisations have also been using controller-to-controller and controller-to-processor Standard Contractual Clauses ('SCCs') under Article 46(2) GDPR to legitimise most of their transfers of personal data to international organisations or third countries. Nowadays, long and detailed data protection contracts are commonplace. However, important inclusions are still left out of such contracts, leaving organisations vulnerable to regulatory action.

This article explains what needs to be included in the various types of data protection contracts based on the positions of the European Data Protection Board ('EDPB') and the UK Information Commissioner's Office ('ICO'), as supported by relevant cases ruled on by the Court of Justice of the European Union ('CJEU').

The importance of agreeing on 'the how'

As seen from guidance and case law issued during the last few months, the first priority in ensuring that a data protection agreement is effective and compliant is discussing and agreeing on the 'how'. This has been highlighted in particular in a controller-processor relationship but clearly applies to joint controller contexts as well. Further, as we have seen in the judgment of the CJEU in the Schrems II case, ensuring that what is in place is effective is also relevant in the terms of Article 46 arrangements and agreeing on the how is, again, a key element to deal with this requirement.

Controller processor agreements

In practice, most agreements between controllers and processors consist of two sections:

- a clause in which the mandatory content set out in Article 28 (3) and (4) of the GDPR are copied into general provisions. Whether these contain a higher or lower level of detail, they tend to be mainly generic and applicable to every possible processing activity; and
- a Schedule in which details of the subject-matter, nature, purpose and duration of the purpose of data processing are defined, along with the type of personal data, categories of data subjects and obligations and rights of controllers.

However, this does not seem to be enough. In its recently issued Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the Danish Supervisory Authority (copy at www.pdpjournals.com/docs/888087), the European Data Protection Board expressly stated that "a contract under Article 28 GDPR should further stipulate and clarify how the provisions of Article 28 (3) and (4) will be fulfilled." The approved version of the controller-processor clauses (copy at: www.pdpjournals.com/docs/888088) offers guidance for organisations seeking to ensure all necessary details are included in contracts. Indeed, the ICO expressly mentions this tool in its controllers-processors guidance, in order to encourage organisations to use them as a valid mechanism that ensures compliance with Article 28 of the GDPR.

In summary, a contract should include the following:

- specific and detailed instructions from the controller — if not in the actual agreement, via regular updates through email (for example). If the latter option is chosen, then this should be made clear in the agreement;
- a thorough evaluation of risks to rights and freedoms to individuals. The controller must provide information to the processor for the processor to be able to understand such risks and take appropriate measures to mitigate them;
- technical and organisational measures implemented by the processor in order to protect the data processed under the controllers' instructions, so the parties can agree on further measures if the controller considers that additional measures should be implemented;
- a list of sub-processors (even if a

'general authorisation' is the option chosen by the controller) and how information on additional sub-processors will be provided to the controller;

- specific instructions concerning international transfers of data by the processor and confirmation of processing locations (e.g. if the parties agree for the data to be processed in specific locations only);
- how and when the processor will notify the controller if aware of a data breach, and what information should be provided;
- how the processor will assist the controller to fulfill each of its relevant obligations;
- how the controller will carry out audits or inspections (e.g. whether by requesting the processor to instruct a third party and share the report with the controller, or for the controller to organise and carry out the audit or inspection);
- whether the processor is obliged under law to keep the personal data for longer than the processing activity instructed, and if so, under which law; and
- agreed contact points for communications between the parties.

In addition, the processor should include a third-party beneficiary clause in its agreements with sub-processors, so the controller can claim against the sub-processor if appropriate (for instance if the processor becomes insolvent).

Practically speaking, although whatever goes into the contract should be decided on a case-by-case basis, the following pointers may assist:

Review existing data protection and information security policies: Doing so may help an organisation to assess how assistance provided by the processor fits into existing procedures. For example, the security measures approved as part of your organisation's policies can be considered for the processor to implement. Alternatively, a processor can agree to confirm an alignment to the level of security and confidentiality set out in the controller's information security policy.

Equally, in order to establish how the processor will assist the controller if a data subject should exercise their data protection rights, direction may be found in the internal steps that your organisation currently takes. If you are a processor, reviewing your existing policies will help to confirm how your organisation will be able to assist the controller.

Ensure effective communication methods are in place: Whilst in some cases providing one email address might be enough for the purposes of the agreement, it is important to ensure that communications are received on time by someone who is able to take immediate action if necessary and in particular when it concerns data breaches. A simple step such as internally setting the email address to be redirected to at least two to four relevant staff or board members ensures that a communication is not missed due to, for example, vacation periods. Parties should also be clear on how to maintain fluent communications and assistance when a situation requires immediate action, as when dealing with certain data breaches.

Join controllers

Identifying joint controller scenarios and having in place the Article 26 arrangements has become relevant given the broad interpretation provided to this term by the CJEU in cases like the Jehovah's Witness case (Case C-25/17). This case dealt with personal data collected by Jehovah's Witnesses during the course of door to door preaching, and the joint controller role of the Jehovah's Witnesses Community. The Fashion ID case (case C-210/16), in which the CJEU considered the position of a fan page used in Facebook, addressed a similar issue in a different context.

The criteria applied in these and other cases of related nature has been summarised by the European Data Protection Supervisor ('EDPS') in his guidelines on the concept of controller, processor and joint controllership (copy at www.pdpjournals.com/docs/888090). Although this guidance is directed at EU Institutions and bodies under the Regulation that applies to them, it is also useful for entities subject to the GDPR due to the similarities and the case law considered in the document.

According to the EDPS guidelines, the decisive elements for joint controllership are:

- each controller has a chance to determine the purposes and the essential elements of the means of a processing operation; and
- a general level of complementarity and unity of purpose, if the purposes and essential elements of the means are jointly determined.

A controller does not need to access nor otherwise process personal data to be considered a joint controller. In the words of the EDPS, a controller will be a joint controller if it 'determines the purposes and means of the processing, has influence on the processing by causing the processing of the personal data to start (and being able to make it stop), or receives the anonymous statistics based on personal data collected and processed by another entity.'

Examples provided include contexts in which different bodies are allocated with different tasks that on the face of things, seem to be developed independently, however, 'neither of the parties involved in the processing operations would be able to achieve the purpose independently'. If, in this context, both parties jointly develop the essential means of the processing operations (for example: the type of data and data subjects required to achieve the purpose or the parties allowed to access the data), then they will be joint controllers.

The ICO has included a checklist in its guidance (copy at www.pdpjournals.com/docs/888089) in order to help organisations with the task of figuring out whether they are joint controllers. The elements stressed are whether the parties involved have a common objective with others regarding the processing; they process data for the same purpose;

(Continued on page 13)

EXAMPLE OF JOINT CONTROLLER CLAUSE

The parties acknowledge that they take joint decisions over the processing of the personal data set out in this clause:

Description	Details
Details	
Definition of joint processing	
Subject matter of joint processing	
Nature, purposes and legal basis of the joint processing	
Definition and type of joint data subjects	
Definition and categories of joint data subjects	

1. In order to ensure compliance with the Data Protection Legislation [this term should be defined in the agreement], the parties agree on the following allocation of responsibilities:
(a) The [company name] is responsible for: [points I to vi to be allocated to one party only if appropriate, or distributed between the parties as appropriate]
(i) Collecting the joint personal data [Include steps agreed]
(ii) Informing joint data subjects as obliged under the Data Protection Legislation [Include steps agreed]
(iii) Implementing appropriate measures to protect the joint personal data [Include measures agreed]
(iv) Being the main contact point for data subjects
(v) Being the main contact point for the ICO
(vi) Informing individuals for the essential elements agreed under this clause
(b) The [company name] is responsible for:
(i) Collecting the joint personal data [Include steps agreed]
(ii) Informing joint data subjects as obliged under the Data Protection Legislation [Include steps agreed]
(ii) Implementing appropriate measures to protect the joint personal data [Include measures agreed]
(iv) Being the main contact point for data subjects
(v) Being the main contact point for the ICO
(vi) Informing individuals for the essential elements agreed under this clause

(2) Regarding the remaining obligations under the Data Protection Legislation, each party shall take steps to ensure compliance in accordance with the level of involvement in the processing of the Joint Personal Data.

(3) Unless agreed otherwise in this clause, the parties agree that in order to deal with issues concerning the processing of personal data, [company name] shall send any communications to [company name] by email, at [email] and [company name] shall communicate with [company name] by email at [email].

(4) The parties shall cooperate in the undertaking of Data Protection Impact Assessments where this is mandatory in relation to the joint processing. [Include steps agreed]

(5) A party will not engage a data processor for the processing of joint personal data unless this is jointly agreed. [Include steps agreed]

(6) A party shall notify the other party immediately (in any event within 24 hours) if it receives any other request, complaint or communication relating to either party's joint obligations under the Data Protection Legislation; receives any communication from the Information Commissioner or any other regulatory authority in connection with joint personal data processed according to this clause; receives a request from any third party for disclosure of personal data where compliance with such request is required or purported to be required by applicable laws; or becomes aware of a data breach, in which case, in addition, it will immediately take internal steps in order to mitigate the breach. [Include immediate steps agreed]

(7) The Parties agree on the following procedures:
(a) To handle joint data subjects' rights requests: [Include steps agreed]
(b) To handle data breaches: [Include steps agreed]
(c) To handle complaints: [Include steps agreed]
(d) To deal with ICO communications: [Include steps agreed]

8) Each party shall, to the extent is it obliged under the Data Protection Legislation maintain complete and accurate records and information to demonstrate its compliance with this clause.

Note: Subscribers can obtain a Word version of this page by sending an email to subs@pdpjournals.com

(Continued from page 11)

they use the same dataset; they have common information management rules; or they have designed the process together.

What might a joint controller arrangements look like?

Article 26(2) of the GDPR states that joint controller arrangements must reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. A clear allocation of the responsibilities is required according to Recital 79 of the Regulation. The key is allocating responsibilities in proportion to the level of involvement and the type of processing activities that each joint controller carries out.

For example, in cases where one organisation does not directly process personal data or have contact with individuals, it will be reasonable to agree that other organisation (which does both) is responsible for ensuring that all processing is carried out in compliance with data protection legislation. Further, that organisation should be responsible for informing individuals of the essence of the joint controller arrangements. In practice, this might consist of an inclusion in its privacy notice that "this activity is carried out in partnership with the other joint controller, and that the one providing the privacy notice is the main contact point and responsible for their processing activities". Such a notice should also include clear information concerning data subjects' rights under the joint controllers processing, or where two organisations are processing individual datasets of personal data in a different manner and for different purposes, the Article 26 clause may be drafted to clarify precisely which task is carried out by each joint controller so the allocation of responsibilities is clear.

When in doubt as to whether or not the parties might be considered joint controllers, organisations should use a more generic type of clause by default. This will help to clarify that despite having a broad objective in common, the processing activities are fully independent, and so each party will be responsible for ensuring compliance with the data processing carried out.

Otherwise, where a joint controller context is clear and, in particular, in cases of complex multi-party projects, organisations should, in line with the approach and guidance seen concerning controller-processors clauses, include details on how each party will deal with their responsibilities and will assist each other. A detailed clause is given as an example on page 12 — subscribers can obtain a Word version by sending an email to subs@pdpjournals.com

The details included in a joint controller clause are not only relevant to ensure compliance with the formal requirements set out in Article 26 GDPR, but also in order to facilitate the calculation of a percentage of liabilities placed on each party, which will assist with the application of Articles 82 (3) and (5) of the GDPR. Articles 26 (3) and 82 (4) provide protections for data subjects to be able to claim against any party involved in the processing, and for each party to be held liable for the entire damage caused to data subjects. So, if one joint controller pays full compensation to data subjects, it will be able to claim back from the other joint controller in accordance with Article 82 (5) and the level of involvement and responsibility that is able to prove. Therefore, if a data subject claims against a joint controller that had a minor level of involvement (or was not involved at all) in the processing activity that caused the damage, it will be easier for this joint controller to prove the extent to which it is entitled to claim back from the other joint controller.

The impact of the Schrems II case ruling

Since the CJEU issued its judgment in the Schrems II case (case C-311/18) in July 2020, EEA organisations are considering how Article 46 Standard Contractual Clauses ('SCCs') could be effectively used to transfer personal data to certain countries. This judgment has implications on every third country to where the data are transferred — not just the US. The EDPB has published a FAQs document and aims to provide more detailed guidance on the use of other mechanisms, such as codes of conducts and certifications. (For a full discussion of this case and its impact, see the article on pages 3-5 of this edition).

Focusing on contractual arrangements — namely the use of SCCs and by extension, intragroup Binding Corporate Rules — it seems that as a minimum, the exporter needs to consider the following:

- carrying out a risk assessment in which the law applicable in the third country is considered;
- assessing whether additional mechanisms can be added to the SCCs (through inclusions to the Annexes). For example, for UK exporters, whether the importer is able to provide information to authorities only if this complies with Article 8 of the Humans Right Act; and
- suspending data transfers if the issue cannot be sorted at the moment. The EDPB is clear on this point, and even states that the contract with the data importer should be terminated if supplementary measures cannot be put in place. Otherwise, the EDPB has stated that the data protection regulator must be notified, which for some organisations might be mandatory as part of their Data Protection Impact Assessment (required under Article 36 (1)).

Conclusion

The principle to bear in mind when it comes to contractual arrangements is simple: every data protection arrangement must explain how each relevant clause will be handled by the parties in practice. Each agreement or template agreement must be tailored to each context. Clarity is important to confirm levels of responsibility and liability placed on each party, so the less legalised and clearer the terms on 'the how' are, the better.

Rocio de la Cruz
Gowling WLG
Rocio.delaCruz@gowlingwlg.com