BCLP. Client Intelligent

Insights

ARE YOU A CONTROLLER, A PROCESSOR OR A JOINT CONTROLLER? SHOULD YOU CARE? NEW EDPB GUIDELINES ON THIS PERENNIAL DATA PROTECTION CONUNDRUM – PART 2

8 October 2020

SUMMARY

On 2 September 2020, the European Data Protection Board ("**EDPB**") published draft guidelines on the concepts of controller, joint controllers and processor, which – as explained below - play a crucial role within GDPR compliance (the "**draft Guidelines**"). These are intended to update and replace decade old guidance and cover the "joint controller" concept brought in by the GDPR.

As well as mainly confirming our understanding of the roles of controller and processor, the draft Guidelines are interesting for their commentary on Article 28 "data processing agreements" (often called "**DPAs**"), which are a prerequisite for every controller and processor relationship. The draft Guidelines also provide the first insights from regulators into what a "joint controller arrangement" is expected to contain.

In Part 1 we covered the guidance on the fundamental concepts. Here we summarise our take on the EDPB's key recommendations on DPAs and joint controller arrangements.

What's in a Name?

"Controllers" must comply with the full range of obligations arising under the GDPR, whereas "processors" operate under the instructions of a controller and, as a result, processors have a much more limited set of obligations to meet. Until an organisation forms a view on its data protection role under the GDPR (e.g. controller, processor, joint controller), it cannot work out which parts of the Regulation apply to its activities, let alone go about complying with those obligations.

This problem is magnified whenever two or more organisations are involved in an interaction where "personal data" is being processed. The intertwined responsibilities and liabilities (including fines of

up to the greater of **4% of annual worldwide turnover/€20 million**) make this much more than a dry legal debate. It is also far from being a new issue.

Our Highlights from the draft Guidelines

We noted the following points from the draft Guidelines (which run to almost 50 pages), grouping them into the main themes:

Article 28 – Data Processing Agreements

- The EDPB considers that a processor **shares responsibility** with the controller for putting in place a compliant Article 28 DPA between them. Previously it was unclear whether the responsibility rested only with the controller.
- Article 28 sets out the minimum requirements but it is not exhaustive. The written agreement between a controller and a processor should not simply restate the language of Article 28 of the GDPR; instead it should provide more specific and concrete information setting out how the requirements of the GDPR shall be met, as well as the level of security which is required. The EDPB's message is that parties entering into DPAs need to ensure that they are **meaningful and relevant documents**.
- The EDPB recommends that there is a specific time frame set out for the processor to notify the controller of a **personal data breach**, e.g. number of hours, after the processor discovers it, and that the contract should specify how the processor should notify.
- The practical management of **data subject requests** can be outsourced to a processor but the responsibility for compliance remains with the controller. The EDPB considers that it is the controller which should be carrying out the assessment as to whether requests are admissible and whether they are being appropriately complied with. This supervision can be on a case by case basis or through detailed instructions to the processor in the contract. Any such outsourcing arrangement does not operate to extend the response time limits (usually one month).
- Where a controller gives **general consent** in the DPA to the processor appointing sub-processors, the EDPB considers that the processor must actively indicate or flag any new sub-processors; it is not sufficient for a processor simply to update an online list which the controller is required to check from time to time.
- The EDPB's view is that the requirement on a processor to **flow down the** "**same" obligations** to sub-processors can be construed in a functional rather than a literal way – this does not require identical language to be used.

- Controllers must only use processors providing **sufficient guarantees** to implement appropriate technical and organisational measures so as to ensure their processing meets the requirements of the GDPR. The EDPB considers that in order to demonstrate such guarantees, the processor may need to share documents such as privacy policies, processing records and less standardised documents, such as those evidencing adherence to an approved code of conduct. Any guarantees should be validated by the controller on an **on-going basis,** including through audits and inspections, where appropriate and at appropriate intervals.

- When a controller is making its **assessment** of a processor's guarantees, it can (and should) take account of a processor's expert knowledge (especially technical), its reliability, its market reputation and its resources.

- The EDPB states that the DPA should include an obligation on the processor to obtain the controller's approval before **changing the security measures** it deploys; the EDPB recommends that the contract contain a notice and approval framework. The EDPB also references the single approved-form DPA, submitted by the Danish supervisory authority last year; however, that document does not include all of the recommendations contained in the draft Guidelines.

Joint controller arrangements

- Article 26(1) of the GDPR requires that joint controllers determine their respective responsibilities "by means of an arrangement between them" which is binding. Achieving a documented 'arrangement' containing a **clear allocation of responsibilities** is essential. The EDPB recommends a written contract or other legally binding act under European Union or Member State law to which the parties are subject.

- Clear allocation of responsibilities is of paramount importance when it comes to who will be responsible for responding to **data subject requests** and publishing GDPR compliant privacy notices.

- The allocation of responsibility should take account of which joint controller is **best positioned to comply** with the specific GDPR obligation. The EDPB recommends that parties should document the relevant factors that have been considered alongside the internal analyses which has been carried out in order to allocate the specific responsibilities.

- No obligatory **form of "arrangement"** is specified, however the draft Guidelines recommend using a written contract or other legally binding act under European Union or Member State law to which the parties are subject. This will provide a transparent means of codifying the parties' respective obligations and also allows the parties to demonstrate their compliance with their obligations, in line with the principle of accountability.

- The draft Guidelines also suggest that the parties should **include the information specified under Article 28(3)** in respect of DPAs within their arrangements, namely the subject matter

and purpose of processing, the type of personal data and the categories of data subjects.

Next steps

The draft Guidelines remain open to public consultation until 19 October 2020. Once finalised, they will provide an important resource to organisations and an important benchmark against which to measure existing agreements and to prepare future ones.

The direction of travel appears to be towards greater complexity and potential confusion. The EDPB's guidance in relation to DPAs and joint controller arrangements seems to envisage that parties will invest greater focus and attention in such documents. That may well be a privacy-enlightened perspective but it will be challenging to implement across the broad range of situations where such agreements are required. For SMEs, in particular, the emergence of standard, approved templates for joint controller arrangements and also additional template DPAs cannot arrive soon enough.

RELATED CAPABILITIES

- Data Privacy & Security
- General Data Protection Regulation

MEET THE TEAM

Geraldine Scali

London

geraldine.scali@bclplaw.com
+44 (0) 20 3400 4483

should not be based solely upon advertisements. This material may be “Attorney Advertising” under the ethics and professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP’s principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.