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 1

1 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.

Part 1 covers the updated commentary on these fundamental concepts. In Part 2, we will cover the EDPB's 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.

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:

Controller

- Only a controller is able to determine the purpose for the processing (the "why"); however, the draft Guidelines specify that when it comes to determining the means of processing (the "how"), this can be split into the **"essential" and "non-essential" means.** Non-essential means (over which processors will typically have control) include practical considerations such as the choice of particular hardware or software or the security measures to be deployed.
- The "controller" concept is a factual one and so all will depend on the circumstances. The EDPB recommends that absent any provisions which confirm that a party acts as a controller, an in-depth analysis may be required in order to determine whether a party "exercises a **determinative influence**" in respect of the processing. As confirmed by EU case law, a party can be a controller even where it does not have actual access to the data.
- It is not possible either to become a controller, or to escape controller responsibilities, simply by shaping the contract in a certain way if the facts indicate something else.
- The imbalance in negotiating power of a small controller with respect to big service providers is not a justification for the controller to accept terms and contracts which are not in compliance with the GDPR.

Processors

- An entity may still be considered a processor where it offers a "**preliminarily defined service**" (i.e. a highly detailed specification of the services) albeit the controller must (still) have the final say in approving how the processing is carried out and/or be able to request changes.
- It is not sufficient for a processor – in particular a big service provider - to modify its processing terms by merely publishing updated terms on its website; the controller should be notified and approve them.
- 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.

Joint controllers

- Joint controllership means that more than one entity holds "**decisive influence**" over whether and how processing takes place. The EDPB notes two forms this could take: either a "**common decision**" (involving the parties "deciding together", where a common intention is evident) or "**converging decisions"** (involving decisions which complement each other and which are necessary for the processing to take place). For converging decisions, the processing requires both parties' participation to be "**inseparable" i.e. inextricably linked**.

- "**Joint" does not mean "equal**" – it is possible to have different entities involved at different stages of processing and to different degrees. The level of responsibility needs to be assessed taking all the circumstances into account. Parties could therefore be joint controllers of a particular stage and independent controllers at another. The flowcharts provided with the draft Guidelines hint at the complexity this could lead to in practice.

- Using a common data processing system or infrastructure does not inevitably equate to a joint controller situation; common or converging decision making is still required for joint controllership to arise.

- 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.

Next steps

The direction of travel appears to be towards greater complexity and with it, unfortunately, a greater potential for confusion. The EDPB hints that further guidance may be required in relation to the nuanced matter of distinguishing between controllers and processors (in particular regarding "essential" and "non-essential" means).

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

In Part 2 of our update, we summarise the EDPB's recommendations for DPAs and joint controller arrangements.

RELATED CAPABILITIES

- Data Privacy & Security
- General Data Protection Regulation

MEET THE TEAM

Geraldine Scali

London

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