



Workday Comments on European Data Protection Board Guidelines 07/2020 on the concepts of controller and processor in the GDPR

October 19, 2020

Workday is pleased to provide feedback on the Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR (the “Guidelines”) proposed by the European Data Protection Board (EDPB). We believe that guidance from the EDPB is vital to helping ensure consistency of application of the General Data Protection Regulation (GDPR) across the EU. Workday is a leading provider of enterprise cloud applications for finance and human resources. Workday is a leading provider of enterprise cloud applications for finance and human resources, helping customers adapt and thrive in a changing world. Workday applications for financial management, human resources, planning, spend management, and analytics have been adopted by thousands of organizations around the world and across industries—from medium-sized businesses to more than 60 percent of the Fortune 50. Headquartered in Pleasanton, California, Workday has more than 12,300 employees worldwide and 21 offices across Europe. Workday’s European-based customers include Airbus, BlablaCar, Deutsche Bank, Primark, Siemens, Sanofi, and ThyssenKrupp.

Importance of Controller-Processor Distinction. Workday is pleased to have this opportunity to provide input on the Guidelines. Given the importance of the concepts of “controller” and “processor,” Workday is pleased the EDPB took this topic up as a priority in its guidance. In addition to improving regulators’ consistent application of these concepts, the guidance also helps companies as they enter into commercial arrangements with one another by establishing a common understanding of how these GDPR concepts are applied, narrowing potential gaps in how companies view their respective roles and the contractual terms needed. Importantly, as the Guidelines recognize, the concepts of “controller” and “processor” are functional concepts.¹ They reflect the actual relationship between the parties in their day-to-day operations, whether or not their agreement specifies something different.

Accountability Principle. At Workday, we believe that privacy is a fundamental right. We are deeply committed to protecting our customers’ privacy. Our [products](#) include features that not only ensure Workday is GDPR compliant, but also [enable](#) our customers to comply with the regulation as well. In our business, Workday most often acts as a data processor with respect to our customers, who are data controllers. As the Guidelines note in their discussion of the accountability principle found in Article 5(2) of GDPR, the controller needs to demonstrate that the processing is performed in accordance with GDPR and assess the processor’s expert knowledge, reliability, and resources.² As a processor, we provide a

¹ European Data Protection Board Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0 (hereinafter “Guidelines”) adopted on 2 September 2020, p. 10.

² *Ibid.*, p. 8.

large amount of information on our security controls, along with SOC audits and other certifications, to help our customers to demonstrate their compliance with GDPR in their use of Workday.

Controllers and the Purposes of Processing. The Guidelines confirm that the controller is the entity that determines the purposes and means of processing. In particular, as they note, it is the controller alone that determines the purposes of processing—the reason *why* processing takes place.³ When an entity chooses to use a cloud computing service, or to use an AI service, it is the one that determines that the service should be used and reasons for processing the data with the service. As Section 3.3.1 of Opinion 05/2012 (WP 196) on Cloud Computing of the Article 29 Working Party states:

The cloud client determines the ultimate purpose of the processing and decides on the outsourcing of this processing and the delegation of all or part of the processing activities to an external organisation. The cloud client therefore acts as a data controller.⁴

Processors and Technological Means. Similarly, the Guidelines note that the controller determines the “essential means.”⁵ Those are by definition high-level—the choice to use a cloud service or an AI application—as in doing so the controller will determine which data will be processed, for how long, and so on. As the Guidelines state, the processor remains free to choose the most suitable technical and organizational means—such as the software used or security measures deployed (subject to Article 32 of GDPR)—without becoming a controller.⁶ “Means” does not equate to “technological design.” Opinion 05/2012 confirms this, stating that “[w]hen the cloud provider supplies the means and the platform, acting on behalf of the cloud client, the cloud provider is considered as a data processor.”⁷

Improving Services at the Direction of the Controller. Importantly, the Guidelines note that an obligation on processors is to process data for the “benefit of the controller.”⁸ Quite clearly this means following the controller’s instructions. But it also means that those instructions can be broad, so long as they are for the controller’s benefit. In many cloud contracts, the controller instructs the processor to process the data in order to improve the service offered to the controller. So long as the controller benefits from the improvements to the service, such an instruction is legitimate, even if the processor is also able to make that improvement available to others. While that may benefit the processor, it is not carrying out the processing for its own purposes, but doing so in compliance with the controller’s instructions and for its benefit.

³ Guidelines, p. 13.

⁴ Article 29 Working Party Draft Opinion 05/2012 on cloud computing adopted July 1 2012, 01037/12/EN, WP 196, p. 7.

⁵ Guidelines, p. 13.

⁶ *Ibid.*, p. 15.

⁷ Article 29 Working Party Draft Opinion 05/2012, WP 196, p. 7.

⁸ Guidelines, p. 24.

Documenting Instructions. As the Guidelines note, the processor must only process data based on documented instructions from the controller.⁹ Most contracts will include a set of instructions. Those can be further supplemented, but the Guidelines seem to assume that the instructions will be given by email or in writing in a way that they can be kept with the contract. In the case of cloud service providers, however, the manner in which a customer chooses to configure the system constitutes an instruction. Consider an expense report tool: it is the customer that chooses to turn on that functionality and defines the approval path required before the expense is approved. Configuration choices are documented, so meeting the requirements of GDPR, but it wouldn't make sense to keep those with the contracts when they are part of the audit trail of the underlying cloud system.

Assisting with Data Subject Requests. Similarly, it is important to clarify that while the processor is required to provide assistance in responding to data subject requests “by appropriate technical and organisational measures, insofar as this is possible” that those technical measures can and do include enabling the controller to extract the data from the service itself.¹⁰ Where the controller itself has access to the requested information, the processor has met its obligation to provide assistance.

* * *

Workday appreciates the opportunity to provide input on the EDPB Guidelines. Please do not hesitate to contact Jason Albert, Managing Director of Public Policy, at ejason.albert@workday.com with any questions or if we can provide further information.

⁹ *Ibid.*, p.34.

¹⁰ *Ibid.*, p. 36.