

GDPR Supplemental Measures Addendum

This frequently asked questions (FAQ) document provides responses to customer queries regarding VMware's GDPR Supplemental Measures Addendum (the Addendum). VMware published the Addendum in light of the Schrems II decision and the revised EU standard contractual clauses (SCCs).

Q. Where can I access the Addendum?

A. The Addendum forms an integral part of VMware's Data Processing Addendum (the DPA). To access the DPA and the Addendum, [click here](#).

Q. What changes does the Addendum introduce?

A. The Addendum supplements VMware's DPA to align it with the revised SCCs requirements. Specifically, the Addendum

- Describes how VMware handles government access requests, including notification obligations to its customers;
- Affirms that VMware has no reason to believe that applicable laws would prevent VMware from fulfilling its notification obligations to customers; and
- Commits to notify customers if VMware believes that it can no longer comply with the above requirements.

Q. When does the Addendum apply? Does it need to be signed?

A. The Addendum automatically applies and becomes part of every new and existing agreement a customer has with VMware, provided such agreement references the DPA. There is no need to sign the Addendum. The Addendum applies to Personal Data (defined in the DPA) within the scope of GDPR.

Q. Where can I find more information about VMware's approach to handling Government Access Requests?

A. [VMware's Principles for Handling Government Requests to Access Customer Content](#) assists customers in further understanding VMware's

commitments and processes for handling government access requests, including commitments set forth in [VMware's Binding Corporate Rules](#).

Q. Does VMware make any contractual commitments on how it handles government access requests?

A. Yes. Sections 2 and 3 of the Addendum supplement in greater detail our contractual commitments set out in the "Required Disclosures" section of [VMware Terms of Service](#):

Where VMware is not legally prohibited from doing so, VMware will:

- **Notify the customer** of any demand for disclosure of Personal Data
- **Refer the Government Agency to the customer;** and
- **Only provide access to Personal Data with the customer's prior authorization.** If the customer requests, VMware will, at the customer's expense, take reasonable steps to contest any access request.

In the event VMware is legally prohibited from notifying the customer, VMware will:

- **Evaluate the legality of any demand for disclosure;**
- **Challenge the order** if it reasonably believes the order does not comply with applicable law, and
- **Limit the scope of any disclosure** to only the information VMware is required to disclose.

In no event will VMware disclose any Personal Data in a massive, disproportionate, and indiscriminate manner that goes beyond what is necessary in a democratic society.

VMware is a global company and is subject to the laws of the various countries in which it operates. The list of countries where Personal Data is processed in relation to a specific Service Offering or Support Services is set forth in the applicable Sub-processor list(s), identified [here](#).

GDPR Supplemental Measures Addendum

Last Revised: November 2021

