

VMWARE PRINCIPLES

For Handling Government Requests to Access Customer Content

VMware may on occasion receive a request from a government agency or law enforcement authority seeking access to content belonging to a customer. This document explains the principles VMware follows if we receive such a request and is intended to assist customers in evaluating our hosted offerings. This document is not legal advice and VMware recommends that its customers consult their own legal counsel to understand legal requirements that may apply to their specific situation.

Protection of Customer Content

VMware is committed to protecting its customers' data while complying with applicable law. VMware has a comprehensive security and privacy program designed to protect customers' data submitted to our services ("Customer Content" or "Your Content"), including personal data ("Personal Data") as such terms are further defined in our [Terms of Service](#). The "Required Disclosure" section of our [Terms of Service](#) outlines how VMware responds to government access requests, our [Data Protection Addendum](#) outlines our commitment to protect Personal Data against unauthorized access or disclosure, and our [Processor Binding Corporate Rules](#) outline our policy for responding to disclosure requests for Personal Data contained in Customer Content.

Steps VMware takes when responding to a request for Customer Content

Regardless of where a request comes from or who the customer is, VMware is vigilant about protecting Customer Content. VMware will not disclose Customer Content unless required to do so to comply with a legally valid and binding obligation or order. VMware reviews each request to determine that it complies with applicable laws. The following sets forth the steps VMware takes when responding to a request for Customer Content, as further set forth in the [Terms of Service](#) ("Required Disclosures" section):

Where Customer Notification is Not Legally Prohibited: VMware will:

- **Notify the Customer:** Notify its customers of any demand for disclosure of Customer Content pursuant to valid legal process unless prohibited or otherwise restricted by law.
- **Refer Government Agency to the Customer:** Inform the relevant government authority, to the extent possible, that VMware is a service provider acting on the customer's behalf and all requests for access to Customer Content should be directed in writing to the contact person the customer has identified to us. If the customer does not provide a contact, we will direct the government agency generally to the customer's legal department.
- **Limit Access:** Only provide access to Customer Content with your authorization. If the customer requests, we will, at the customer's expense, take reasonable steps to contest any required disclosure.

VMWARE PRINCIPLES

For Handling Government Requests to Access Customer Content (Cont.)

Where Customer Notification is Legally Prohibited: In the event VMware is legally prohibited from notifying the customer of a government request for access to Customer Content, VMware will:

- Evaluate Legal Validity: Review each government request for Customer Content and evaluate whether the request is legally valid and binding. We take into account all applicable laws when reviewing the lawfulness of a government request.
- Challenge any Unlawful Request: Challenge any requests for disclosure of Customer Content if VMware reasonably believes the request does not comply with applicable law.
- Require Legal Process to be Followed: Require governmental agencies to follow appropriate legal process under applicable laws.
- Limit Scope of Disclosure: Limit the scope of any disclosure to only the information we are required to disclose and disclose the information in accordance with applicable law.

VMware's Processor Binding Corporate Rules contain specific requirements regarding our handling of government requests for Personal Data

VMware's policy is that the customer should have the opportunity to protect any personal information included in Customer Content because the customer has the greatest interest in opposing, or is in the better position to comply with, a disclosure request. If VMware receives a legally valid and binding request for disclosure of Personal Data governed by VMware's Processor Binding Corporate Rules ("BCRs"), VMware will, after assessing the nature, context, purposes, scope and urgency of the request:

- Notify the Customer: Notify the Customer promptly unless prohibited from doing so by law or where an imminent risk of serious harm exists that prohibits prior notification.
- Notify Data Protection Authorities: Put the request on hold in order to notify and consult with the competent Data Protection Authorities for the customer unless legally prohibited. If prohibited from notifying the Data Protection Authorities, VMware will use its best efforts to inform the requesting authority about its obligations under applicable data protection law and to obtain the right to waive the prohibition about notifying the Data Protection Authority.
- Annual Disclosure: Where VMware is not in a position to notify the competent Data Protection authority of the request, VMware commits to preparing an annual disclosure overview and to make this disclosure overview available upon request to competent Data Protection Authorities.

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