Data Processing Agreement for Jamf Customers
Frequently Asked Questions ("FAQ")

We are committed to maintaining the privacy and security of your data. To help you develop a better understanding of our Data Processing Agreement for Jamf Customers ("**DPA**"), we have put together this FAQ to answer some of the most asked questions. Capitalized terms used, but not defined in this FAQ, are defined in the DPA or Jamf's Software License and Services Agreement ("**SLASA**"). This document is provided for informational purposes only and should not be considered legal advice. It will not become part of your contract with Jamf.

What is the DPA and how is it made available to customers?
The DPA is an agreement between Jamf and our customers that regulates the Processing of Personal Data you provide to us. It is used when Data Protection Laws apply to our Processing of Personal Data when providing services to you. The DPA sets out the Parties' legal obligations and commitments related to Processing Personal Data. Our DPA is incorporated by reference into our SLASA and is accepted when you accept our SLASA. It can be found at: https://resources.jamf.com/documents/Jamf-Customer-DPA.pdf.

Who is the Controller and who is the Processor?
With respect to Personal Data you provide through our Product Offerings, you are the Controller, and we are the Processor. As the Processor, we do not make independent decisions about Personal Data and only Process it upon your instructions and in accordance with our SLASA, DPA, and Data Protection Laws.

What does the DPA cover?
The DPA explains how we fulfill our obligations under Data Protection Laws. In the DPA you will find the following information and commitments:

- The categories of Personal Data that we may process for customers. We do not have access to all Personal Data on your Devices, only what is needed to manage and secure your Devices. Schedule 1 contains the details of Processing, including the duration, nature, and type of data being Processed.
- How we can assist you with responding to Data Subject requests and conducting data protection impact and transfer impact assessments https://resources.jamf.com/documents/Jamf-TIA.pdf.
- The technical and organizational security measures we have implemented to protect Personal Data are set out in Schedule 3.
- How we maintain the confidentiality of your Personal Data by ensuring that all personnel with access to Personal Data are committed to confidentiality as part of their employment with us.
- How our Sub-Processors are contractually obligated to meet the same data protection obligations that we provide to our customers. We do this by conducting security assessments prior to onboarding Sub-processors and having appropriate contracts in place to ensure the confidentiality and protection of Personal Data.
- How we notify you of any changes to Sub-processors and how you can object to the use of a new Sub-processor using the procedure set out in the DPA. You can find a list of Jamf Sub-processors in Schedule 2.
- Our security incident management policies and procedures and the requirement to notify you within 72 hours if a Personal Data Breach affecting your Personal Data occurs.

For more information, please see https://www.jamf.com/trust-center/privacy/>.

Why can't Jamf use my organization's DPA?
Our DPA is specific to our Product Offerings and covers the processes we use to ensure that we meet our obligations under Data Protection Laws. Like many global software companies with tens of thousands of customers, we maintain a consistent and comprehensive set of security practices, certifications, notification policies, and sub-processing activities which are reflected in the DPA and tailored to our Product Offerings and Services. We use our DPA to contract efficiently with our customers, however, upon request we will respond to security and audit questionnaires to confirm that we are meeting our obligations with respect to the security of Personal Data. You can read more about this on the Jamf Trust Center.

What is the transfer mechanism used for the transfer of Personal Data outside the EEA, UK, or Switzerland to the United States?
We rely on approved and applicable Standard Contractual Clauses "**SCCs**" that are incorporated into our DPA and form a part of the contract between you and Jamf. We are also certified as a participant in the EU-U.S. DPF, which replaced the EU-U.S. Privacy Shield. The DPA includes a provision related to addressing a situation in which any approved SCCs are replaced or superseded. We are committed to ensuring appropriate transfer mechanisms are in place with our customers.

Why aren't the SCCs attached to the DPA?
Given the length of the SCCs, we have chosen to incorporate the SCCs by reference into the DPA. Customers may execute the SCCs separately following the procedure set out in the DPA.

Will Jamf add the docking clause of the SCCs to the DPA?
We do not include the docking clause by default; however, we may consider it to be added in certain circumstances, see Section 4 (c) of the DPA.

What certifications does Jamf hold that demonstrate a commitment to protecting your Personal Data?
We maintain a SOC 2 Type II for our Product Offerings and are ISO 27001 and ISO 27701 certified. Please visit the Security Portal and Compliance pages on the Jamf Trust Center for more information about our certifications and to review our SOC 2 reports.

Has Jamf appointed a Data Protection Officer?
Yes. We have appointed a Data Protection Officer (DPO) in the European Union/United Kingdom who can be contacted at privacy@jamf.com. This email address can also be used as the contact for any queries relating to the DPA.

Where will the Personal Data provided to Jamf be geographically located?
Location details are set out in our Sub-processor documentation, available in Jamf's Trust Center.

We use data centers for core Hosted Services in the U.S. (East, West, Government), Germany, United Kingdom, Japan, Australia, and Ireland. Personal Data will typically reside in a data center consistent with the customer's geographical region, except if a data center is not available in that location. For example, Personal Data of a U.S. customer will reside in the U.S., when possible, whereas Personal Data of a customer in the European Union will reside either in Germany, Ireland, or the United Kingdom (whichever is preferred by the customer and available for the Hosted Service).

For Hosted Services where the customer can select the geographic region, Jamf will not move the customer's Hosted Services instance to another geographic region without the customer's consent. For example, if you select the AWS German data center for your hosting location it will remain in there unless you request that it be moved to a different region. Please review our Sub-processor information page to see current Hosted Services locations.

How does Jamf use Sub-Processors?
Our Sub-processors provide cloud infrastructure and other services to assist us with providing the Hosted Services and other Product Offerings to customers. We impose written data protection obligations on our Sub-processors that offer at least the same protection of Personal Data to which we have committed to for our customers. You can access information about our Sub-processors on the Jamf Sub-processors page.

Does the DPA address compliance obligations under the CPRA?
Yes. Our DPA contains specific provisions to comply with the CPRA, which is a similar regime to GDPR. If you are **not** subject to the CPRA, then the CPRA provisions contained in the DPA simply will not apply to you.

Does the DPA address compliance obligations under Data Protection Laws other than those specifically listed in this FAQ?
Yes. Our definition of "Data Protection Laws" is very broad and includes all applicable data protection, privacy, and cybersecurity laws, rules, and regulations of **any** country. Therefore, the laws of countries in which we do business, will be applicable. Specific jurisdictions are set out in further detail to ensure compliance with contractual commitments required for data processing agreements in those countries. Section 4 of the DPA further prescribes the considerations in play when we Process your Personal Data, which includes Processing Personal Data in accordance with Data Protection Laws; therefore, where other Data Protection Laws are applicable, we are committed to complying with them.

What happens if Jamf receives a request from a government entity to access a customer's Personal Data?
We protect our customers' privacy and do not voluntarily provide access to any customer data. We may occasionally receive a request from a government agency or law enforcement authority seeking access to data belonging to a customer. We are not the owner of customer Personal Data and, accordingly, if we receive a government request for customer data, if permitted by law, we try to refer the request to the affected customer so that the customer can work directly with the governmental agency to respond. We do not disclose customer data to government agencies unless compelled by law and we also challenge unlawful requests.

As of the date this FAQ was last updated, we have not received requests under U.S. surveillance laws to provide Personal Data to the U.S. government. Section 4 g) of the DPA specifically outlines the supplementary measures we will take if we receive a Government Agency request.

What happens to my Personal Data after I stop using Jamf's Product Offerings?
After termination or expiration of the agreement (and DPA), your Personal Data will be retained for a period of 90 days, after which it shall be deleted or returned (if applicable) in accordance with the procedures and timeframes in the DPA.

Can a customer audit Jamf?
Yes. We will cooperate with you and contribute to audits to check compliance with Data Protection Laws and the DPA. This may include inspections, where we are permitted to allow access, conducted by you or an external auditor engaged by you. There are certain restrictions on audits set out in Section 11 of the DPA.

Can Jamf complete a DPIA for a customer?
We provide resources to assist you with completing data protection or privacy impact assessments when they are required under Data Protection Laws. These are available in Jamf Trust Center . We will also provide you with reasonable assistance to complete a data protection impact assessment or privacy impact assessment, on request.

What if I have additional questions not answered in this FAQ?
If you have additional questions, please go to the Jamf Trust Center where you can find more information or contact your sales representative.