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

Jamf is committed to maintaining the privacy and security of our customers' data. This FAQ is designed to help you understand the Data Processing Agreement for Jamf Customers ("**DPA**") and to provide you an overview of Jamf's DPA and its purpose. **This FAQ is for informational purposes only, should not be considered nor is a substitute for legal advice, and will not be incorporated into or become part of your contract with Jamf**. Certain defined terms used, but not defined in this FAQ, are defined in the DPA or Jamf's Software License and Services Agreement ("**SLASA**").

What is the DPA?
The DPA is a legally binding agreement between Jamf and a Customer that regulates the Processing of Personal Data and covers customers globally. It is used and applicable when Data Protection Laws apply to a Customer's use of Jamf's Services to Process Personal Data and it sets forth the Parties' legal obligations and commitments related to Processing Personal Data. Jamf's DPA is incorporated by reference into Jamf's SLASA and therefore is accepted when a Customer accepts our SLASA.

Which Jamf entity is a party to the DPA?
The contracting entity to the DPA is JAMF Software, LLC, and its Affiliates. Jamf has registered entities in Europe and other countries; however, both the DPA and Jamf's SLASA are entered into with JAMF Software, LLC.

How does Jamf meet its obligations under GDPR?
Protecting the security and privacy of Personal Data is a priority for Jamf. Jamf has a skilled and committed Information Security team dedicated to delivering and maintaining a comprehensive security program. That team, along with Jamf's Enterprise Risk and Compliance team (which includes a team dedicated to privacy compliance) and Legal team, works to ensure compliance with Data Protection Laws, including GDPR and supplementary national data protection laws in the EU, EEA, and/or UK, and that Jamf meets industry standards and best practices for data processing.

Jamf understands that customers may be subject to compliance obligations under Data Protection Laws, including GDPR and UK GDPR. As the data processor, Jamf has implemented robust technical and organizational security measures to protect Personal Data and assist customers in meeting their compliance obligations. This may include helping customers respond to data subject requests and conduct data protection impact and transfer impact assessments.

Jamf regards all Personal Data as confidential and ensures that all Jamf personnel with access to Personal Data are committed to confidentiality as part of their employment with Jamf.

Jamf's Sub-processors undergo rigorous security assessments. Jamf conducts thorough due diligence prior to onboarding Sub-processors to ensure that we can meet our security obligations to customers, including having appropriate contracts in place to ensure the confidentiality and protection of Personal Data. Jamf will notify customers if we change Sub-processors.

Jamf maintains security incident management policies and procedures and will notify you without undue delay if a data breach affecting your Personal Data occurs and provide relevant details to you to assess any impact it may have upon you.

Jamf has applied a Privacy by Design approach to our internal processes, including product design and development, vendor selection and management, and around our Hosted Services. Our commitment to this approach helps us to proactively identify, evaluate, and implement full lifecycle protection over new Personal Data collection and use cases and any changes to existing collection and use practices. For example, Jamf reviews functionality changes to our products for Personal Data impacts and assesses them to determine the level of risk, impact, and necessary control implementation. This allows us to ensure we are only processing Personal Data in accordance with our SLASA, DPA, and a Customer's documented instructions.

Jamf's formal and comprehensive security program is detailed in its independent third-party SOC 2 audit reports and DPA. In addition, Jamf is ISO 27001, ISO 27701, and Cyber Essentials certified. Please contact your Jamf representative if you require further information regarding Jamf's SOC 2 reports and ISO 27001, ISO 27701, and Cyber

Essentials certifications. In addition, Jamf participates in the EU-U.S. Data Privacy Framework ("**EU-U.S. DPF**"). You can learn more about Jamf's certifications via the Jamf Trust Center.

To ensure that Jamf consistently meets its obligations under Data Protection Laws, Jamf does not agree to individual customer security policies. Like many global software/hosted services companies with tens of thousands of customers, Jamf needs to maintain a consistent and comprehensive set of security policies to ensure appropriate protections and consistency in its approach for all customers. However, upon request Jamf will respond to security and audit questionnaires to confirm that Jamf is meeting its obligations with respect to the security of Personal Data. Jamf Customers can obtain additional information via the Jamf Trust Center.

Who is the controller and who is the processor?
With respect to Personal Data provided to Jamf in relation to Customer's use of Jamf's Services, the Customer is the controller and Jamf is the processor. As the processor, Jamf does not make independent decisions about Personal Data and only processes it upon Customer's instructions and in accordance with our SLASA, DPA, and Data Protection Laws.

What is the transfer mechanism used for the transfer of Personal Data outside the EEA, UK, or Switzerland to the United States?
The transfer mechanism upon which Jamf relies for the transfer of Personal Data outside the EEA to the United States (or a country for which an adequacy decision has not been made), is use of the standard contractual clauses approved by the European Commission and annexed to the European Commission's Implementing Decision 2021/914 dated June 4, 2021 ("**EEA SCCs**"). The EEA SCCs are incorporated into our DPA. To further demonstrate our commitment to privacy, Jamf is certified as a participant in the EU-U.S. DPF, which replaced the EU-U.S. Privacy Shield.

The EEA SCCs do not, on their own, govern Personal Data transfers originating in the UK. However, the Information Commissioner's Office issued the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses under section 119A(1) of the UK Data Protection Act 2018, which became effective March 21, 2022 ("**UK Addendum**"). The UK Addendum is incorporated into Jamf's DPA to provide a legal basis for the transfer of Personal Data outside the UK to the United States (or another country for which the UK has not issued an adequacy decision). In addition, Jamf is monitoring the commitment between the UK and U.S. to establish the UK Extension to the EU-U.S. Data Privacy Framework ("**UK Extension**"). Jamf intends to self-certify to the UK Extension as a further demonstration of Jamf's commitment to privacy.

The EEA SCCs, subject to modifications and amendments prescribed by the Swiss Federal Data Protection and Information Commissioner, govern Personal Data transfers to the United States when the Personal Data originates in Switzerland. In addition, Jamf complies with the Swiss-U.S. Data Privacy Framework ("**Swiss-U.S. DPF**") demonstrating Jamf's commitment to privacy.

The DPA includes a provision related to addressing a situation in which the EEA SCCs, UK Addendum, or Swiss Standard Contractual Clauses are replaced or superseded. Jamf is committed to ensuring appropriate transfer mechanisms are in place with its customers. Jamf maintained its Privacy Shield certification to further demonstrate its ongoing commitment to protecting our customers' Personal Data and is now compliant with the EU-U.S. DPF and the Swiss-U.S. DPF and will certify to the UK Extension as evidence of our strong commitment to data protection.

What is contained in the Schedules to the DPA?
Schedule 1 contains the Details of Processing, including a) the List of Parties, b) the Description of Transfer and c) a reference to the competent supervisory authority (all consistent with Annex I to the EEA SCCs).

Schedule 2 contains a link to access a list of Jamf's current approved sub-processors - Jamf sub-processors.

Schedule 3 sets forth details related to the technical and organizational security measures Jamf takes to prevent the unauthorized or unlawful processing or accidental loss, destruction, or damage to Personal Data, which are applicable to all Jamf Customers and designed to ensure that Jamf's processing of Personal Data is done in accordance with applicable Data Protection Laws.

Has Jamf appointed a Data Protection Officer?
Yes. Jamf has appointed a Data Protection Officer in the European Union/United Kingdom who can be contacted at privacy@jamf.com for matters relating to the DPA and privacy. The privacy@jamf.com inbox is monitored constantly. Jamf's general privacy contact can also be reached via the privacy@jamf.com email address.

Where will the Personal Data provided to Jamf be geographically located?
Jamf uses data centers to provide Hosted Services. Certain Hosted Services allow for regional data storage, while others do not. One of Jamf's Hosted Services allows for regional data storage except for certain functionality that only allows for storage in one region. These details are clearly specified in our Sub-processor documentation, available in Jamf's Trust Center.

Current regions in which Jamf utilizes data centers for Hosted Services, that are considered core services, include the United States (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 where the Hosted Service is not available in that country or region. For example, Personal Data owned by a United States customer will reside in the United States, when possible, whereas Personal Data owned by 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 (which is not the region selected by the customer) without the consent of the customer. For example, if you elect for your instance of Jamf Pro to be set up in the AWS German data center, such instance will remain in the German data center unless you request that it be moved to a different region utilized by Jamf. Please reference your Jamf product's Sub-processor's documentation to see the most current Hosted Services locations.

What does a Sub-processor do for Jamf?
Jamf Sub-processors provide cloud infrastructure and other services in various geographic regions that Jamf utilizes to provide Services to Jamf's customers. Jamf imposes written data protection obligations on its Sub-processors that offer at least the same protection of Personal Data to which Jamf has committed to for its customers. You can access information about Jamf's Sub-processors here - Jamf Sub-processors. The Jamf Sub-processors page allows you to access specific Sub-processor information based upon each Jamf product.

Does the DPA address compliance obligations under the CPRA?
Yes. Jamf's DPA contains specific provisions to comply with the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 ("**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. Jamf's 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 forth 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 Jamf Processes a Customer's Personal Data, which includes Processing Personal Data in accordance with Data Protection Laws; therefore, where other Data Protection Laws are applicable, Jamf is committed to complying with them.

What about the main agreement between the parties?
The DPA supplements the SLASA, which is the main agreement between Jamf and the Customer under which Jamf provides Software and Services to the Customer. When the SLASA is accepted by you, the DPA forms part of the SLASA.

Why can't I, as the Customer, use my own data processing agreement?
Jamf has tens of thousands of customers globally and has standardized its approach to data processing terms for all customers, as set out in the DPA. As is the same for most global software/hosted services providers, it is not scalable to review and negotiate individual customer data processing agreements. Jamf's DPA had been drafted to comply with applicable Data Protection Laws, **including but not limited to**, GDPR, UK GDPR, the Swiss Federal Act on Data Protection, and CPRA and is specifically tailored to Jamf's practices and policies. Jamf takes its obligations under Data Protection Laws and the protection of Personal Data very seriously. Jamf constantly monitors the legal landscape related to data privacy and security to ensure Jamf's compliance with Data Protection Laws and fulfill its obligations to Jamf's customers.

Is Jamf obliged to provide or give access to Personal Data to third parties based on national laws?
Jamf protects customer privacy and Jamf does not voluntarily provide access to any data provided to Jamf by customers, specifically including Personal Data. As of the date this FAQ was last updated, Jamf has not received requests under U.S. surveillance laws to provide Personal Data to the U.S. government. Jamf's DPA specifically outlines the supplementary measures it will take in the event Jamf receives a Government Agency Request in Section 4 g) of the DPA and Clause 15 of the EEA SCCs. Additional information is available in the Jamf Trust Center.