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

At Jamf, we are committed to and serious about 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 the SLASA (both defined below).

What is the DPA, and do I need to sign Jamf's DPA?
The DPA is a legally binding agreement entered into by Jamf and a Customer that regulates the processing of Personal Data. 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' obligations related to processing Personal Data. The DPA must be signed by a Customer representative authorized to contractually bind the Customer to a legal document. The DPA is set up to be signed by the Customer in two places - the main body of the DPA will be signed by Jamf and the Customer, and Schedule 1 needs to be signed by the Customer's data protection officer or representative. The latter signature is a requirement relating to the EEA SCCs (Schedule 4 to the DPA) and is already signed by Jamf's data protection representative. Schedule 5 (UK Addendum) to the DPA also includes a signature block but is deemed executed due to the above-referenced signatures and accordingly does not need to be signed.

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 Software License and Services Agreement ("**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 passionate Information Security team dedicated to delivering and maintaining a comprehensive security program. That team, along with Jamf's Compliance team, works to ensure compliance with Data Protection Laws, including the 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 our Customers are 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 not only protect Personal Data but to assist our Customers in meeting their compliance obligations (including Customer responses to data subject requests or conducting data protection 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 subprocessors undergo rigorous security assessments. Jamf conducts thorough due diligence prior to onboarding subprocessors to ensure that we can meet our security obligations to our Customers, including having appropriate contracts in place to ensure the confidentiality and protection of Personal Data. Jamf will provide Customers with notice if we change subprocessors, in accordance with the DPA.

Jamf maintains security incident management policies and procedures and will notify Customer 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 our customers' 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 certified. While the current scope of this certification doesn't cover all Jamf's

products and locations, we continuously work to ensure all people, processes and tools are covered under our Information Security Management System ("**ISMS**"), and we are in the process of expanding our scope to include all Jamf cloud Services. Please contact your Jamf representative if you require further information regarding Jamf's SOC 2 reports and ISO 27001 certification. In addition, 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 Jamf's 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 the Personal Data and only processes it upon Customer's instructions and in accordance with our SLASA, DPA and Data Protection Laws.

What is the legal basis for the transfer of Personal Data outside the EEA or the UK to the United States?
The legal basis for the transfer of Personal Data outside the EEA to the United States (or another country for which an adequacy decision has not been made), is use of the standard contractual clauses approved by the European Commission in Commission Decision 2021/914 dated June 4, 2021 ("**EEA SCCs**"). The EEA SCCs are incorporated into our DPA at Schedule 4.

The EEA SCCs do not govern Personal Data transfers originating in the UK. However, the Information Commissioner's Office ("**ICO**") issued the UK Addendum to the EEA SCCs under section 119A(1) Data Protection Act 2018, which became effective March 21, 2022 ("**UK Addendum**"). The UK Addendum is incorporated into Jamf's DPA at Schedule 5 to provide a legal basis for the transfer of Personal Data outside the UK to the United States (or another country for which an adequacy decision has not been made).

The DPA includes a provision related to addressing a situation in which the EEA SCCs or UK Addendum are replaced or superseded. Jamf is committed to ensuring appropriate transfer mechanisms are in place with its customers. In addition, Jamf has maintained its Privacy Shield certification to further demonstrate its ongoing commitment to protecting our Customers' Personal Data.

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 Subprocessors.

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.

Schedule 4 contains the EEA SCCs that provide a mechanism for the transfer of Personal Data to processors established in third countries that do not ensure an adequate level of protection of Personal Data. The EEA SCCs have been approved by the European Commission as adducing adequate safeguards for restricted transfers (transfers that would be prohibited by Data Protection Laws in the absence of the EEA SCCs). The EEA SCCs are specific to Personal Data transfers out of EEA countries. Note: the Annexes to the EEA SCCs reference the appropriate DPA Schedules to ensure information required by the EEA SCCs is included.

Schedule 5 contains the UK Addendum, which provides a mechanism for the transfer of Personal Data originating from the UK to processors established in third countries that do not ensure an adequate level of protection of Personal Data. The UK Addendum has been issued by the Information Commissioner and was designed to be appended to the EEA SCCs to ensure appropriate safeguards for the transfer of UK Personal Data. Note: Table 1 (Parties) in the UK

Addendum references the DPA and applicable schedules to ensure information required by the UK Addendum is included.

How do modifications to the Jamf DPA with respect to the UK Addendum affect me if I am a current Jamf customer or a potential customer?
Current Jamf Customers that have entered into a DPA with Jamf and who provide UK Personal Data to Jamf for processing can rely on the Standard Contractual Clauses approved by the European Commission in Commission Decision 2010/87/EU, dated February 5, 2010 ("**Old SCCs**") until March 21, 2024. As the data controller/exporter, current Jamf Customers have an obligation to ensure that an appropriate method to transfer UK Personal Data – the UK Addendum – is in place by March 21, 2024, to ensure compliance with applicable Data Protection Laws.

Potential Jamf Customers that become actual Jamf Customers after March 21, 2022, but before September 21, 2022, can rely on the Old SCCs. However, Jamf's DPA currently includes the UK Addendum for immediate use with new customers, which avoids the need to enter an amended or new DPA before March 21, 2024.

Has Jamf appointed a Data Protection Officer?
Jamf has reviewed its obligations under Data Protection Laws and has determined that Jamf does not currently meet the criteria to necessitate the appointment of a specific Data Protection Officer. Jamf has appointed a privacy officer who can be contacted at privacy@jamf.com for matters relating to the DPA. The privacy@jamf.com inbox is monitored constantly. Jamf will continue to monitor its obligations regarding the appointment of a Data Protection Officer and will appoint a Data Protection Officer if required by applicable Data Protection Laws.

Where will the Personal Data provided to Jamf be geographically located?
Jamf uses data centers to provide Jamf cloud Services. Current regions in which Jamf utilizes data centers include the United States (East, West, Government), Germany, London, Japan, Australia, Netherlands, Ireland, Hong Kong, Spain, Italy, India, Norway, France, Mexico, Brazil, South Korea, Singapore, Canada, and Switzerland. 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, London, or Ireland (whichever is preferred by the Customer and available for the service). With respect to Jamf's provision of certain hosted services, once a Customer has selected a geographic region in which the Customer's instance of hosted services will be set up, Jamf will not move the Customer's instance to another geographic location. For example, if a Customer elects for its instance of hosted services to be set up in the AWS German data center, such instance will remain in that data center unless the Customer requests that it be moved to a different region utilized by Jamf.

What does a sub-processor do for Jamf?
Jamf subprocessors 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 subprocessors that offer at least the same protection of Personal Data to which Jamf has committed to for its customers. You can access a current listing of Jamf's subprocessors here - Jamf Subprocessors. The Jamf Subprocessors page lists our subprocessors together with the basic information on the services they provide to Jamf and which services are utilized with specific Jamf products.

Does the DPA address compliance obligations under the CCPA?
Yes. Jamf's DPA contains specific provisions to comply with the California Consumer Privacy Act ("**CCPA**"), which is a similar regime to GDPR. If you are not subject to the CCPA, then the CCPA provisions contained in the DPA simply will not apply to you.

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 signed by the parties, 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 GDPR, UK GDPR, and CCPA 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 the privacy of our customers and Jamf does not voluntarily provide access to any data provided to Jamf by Jamf's 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 (see Section 4 e) of the DPA and Clause 15 of the EEA SCCs).