Data Transfer Impact Assessment

This document is designed to provide information to assist Jamf customers with conducting data transfer impact assessments in connection with their use of Jamf products, considering the Schrems II ruling of the Court of Justice of the European Union and the European Data Protection Board's related recommendations.

This document describes the legal regimes applicable to Jamf in the United States ("US"), the safeguards Jamf puts in place in connection with transfers of customer personal data from the European Economic Area ("EEA"), United Kingdom ("UK") or Switzerland, and Jamf's ability to comply with its obligations as "data importer" under the relevant personal data transfer mechanisms – the EEA Standard Contractual Clauses ("EEA SCCs") or the UK Addendum.

Jamf safeguards the personal data our customers entrust us to process, particularly when circumstances require that we transfer that personal data to a third country lacking an adequacy decision — whether for the purposes of support, Hosted Services, or security review.

Where the customer is the controller of the data, Jamf may transfer customer's personal data outside of the customer's primary region to provide our services. For example, Jamf provides support and hosted services with staff from various countries around the world. Jamf employees may need to access personal data to provide these services. In a few circumstances, we may utilize vendors (as sub-processors to Jamf) outside our customers' primary regions.

The transfer impact assessment information below identifies and describes the risks associated with data transfers of personal data to third countries lacking an adequacy decision, as well as any supplementary measures we have taken — or have required our vendors to take — to safeguard personal data. Please see our Data Processing Agreement for Jamf Customers ("DPA") for additional details, such as the nature of the processing or the retention period of the data. In all cases, the categories of data subjects are the employees of Jamf customers (or students of Jamf customers if the customer is an education customer).

For additional resources about Jamf's Software License and Service Agreement, DPA, and Privacy program, please visit Jamf's Trust Center. Our list of sub-processors is available in the Trust Center.

Transfer Impact Assessment

Jamf's DPA incorporates the EEA SCCs. In response to the heightened requirements created by the Schrems II decision the European Commission adopted the EEA SCCs, which require a data importer (Jamf in this case) to provide specific information about personal data transfers it undertakes, and requires the parties to conduct a transfer impact assessment to evaluate risks involved with the transfer of personal data to countries outside the EEA. The EEA SCCs also require the parties to take into account any relevant contractual, technical and organizational safeguards to supplement the safeguards set forth in the EEA SCCs.

Please refer to Schedule 1 of the DPA for a description of personal data transfers, including the nature of Jamf's processing activities in connection with the provision of the services, the types of customer personal data transferred, and the categories of data subjects.

Please refer to Schedule 3 of the DPA to review the security measures Jamf has implemented to protect the personal data of our customers' data subjects.

Transfer of data to the US

In response to Schrems II, the European Data Protection Board (EDPB) has made clear that Binding Corporate Rules and approved standard contractual clauses remain valid data transfer mechanisms. As the EDPB states in its guidance, however, transfer mechanisms do not operate in a vacuum, and may need to be paired with supplementary measures that enhance protection of personal data.

EU data storage

Most Jamf products have the option for customers to choose where their data is stored, including an option in the EEA. However, Jamf may need to process this data in other countries to support our customers, to provide our hosted services, and conduct security incident reviews.

Jamf Now is the only product that does not allow for regional data storage; all data is stored in the US.

US Surveillance Laws

Is Jamf subject to FISA 702 or EO 12333?

Jamf, like most US-based SaaS companies, could technically be subject to FISA 702 where it is deemed to be a remote computing service provider ("RCSP"). However, Jamf does not process personal data that is likely to be of interest to US intelligence agencies.

Furthermore, Jamf is not likely to be subject to upstream surveillance orders under FISA 702, the type of order principally addressed in, and deemed problematic by, the Schrems II decision. Jamf does not provide internet backbone services, but instead only carries traffic involving its own customers. To date, the US Government has interpreted and applied FISA 702 upstream orders to only target market providers that have traffic flowing through their internet backbone and that carry traffic for third parties (i.e., telecommunications carriers).

EO 12333 contains no authorization to compel private companies (such as Jamf) to disclose personal data to US authorities and FISA 702 requires an independent court to authorize a specific type of foreign intelligence data acquisition which is generally unrelated to commercial information. If US intelligence agencies were interested in the type of data that Jamf processes, safeguards such as the requirement for authorization by an independent court and the necessity and proportionality requirements would protect data from excessive surveillance.

What is Jamf's experience dealing with government access requests?

To date, Jamf has never received a US National Security Request (including requests for access under FISA 702 or direct access under EO 12333) in connection with customer personal data.

Therefore, while Jamf may technically be subject to the surveillance laws identified in Schrems II we have not been subject to these types of requests in our day-to-day business operations.

Jamf Services' Processing Locations

Products & Services	Countries where Jamf stores Customer Personal Data	Countries where Jamf processes Customer Personal Data
Jamf Connect	N/A	N/A
Jamf Now	United States	Australia, Czech Republic, Japan, Netherlands, Poland, United States
Jamf Pro	Australia, Germany, Japan, United Kingdom, United States (location chosen by Customer)	Australia, Czech Republic, Japan, Netherlands, Poland, United States
Jamf Protect	Australia, Germany, Japan, United Kingdom, United States (location chosen by Customer)	Australia, Czech Republic, Japan, Netherlands, Poland, United States
Jamf School	Germany, Japan, United States (location chosen by Customer)	Australia, Czech Republic, Japan, Netherlands, Poland, United States

Jamf Data Policy, Private Access, Threat Defense, Safe Internet– core data centers	Ireland	Australia, Czech Republic, Japan, Netherlands, Poland, United Kingdom, United States
Jamf Data Policy, Threat Defense, Safe Internet – edge data centers chosen by the Customer where available for various services	Australia, Belgium, Brazil, Canada, Finland, France, Germany, Hong Kong, India, Ireland, Italy, Japan, Mexico, Netherlands, Norway, Singapore, South Africa, South Korea, Spain, Sweden, Switzerland, United Kingdom, United States	Australia, Czech Republic, Japan, Netherlands, Poland, United Kingdom, United States
Jamf Private Access – edge data centers chosen by the Customer where available for various services	Australia, Brazil, Canada, Germany, India, Ireland, Japan, Singapore, South Africa, United Kingdom, United States	Australia, Czech Republic, Japan, Netherlands, Poland, United Kingdom, United States
Jamf Data Policy, Private Access, Threat Defense, Safe Internet - optional email services (Mailchimp, Twilio)	United States	Australia, Czech Republic, Japan, Netherlands, Poland, United Kingdom, United States

Onward transfers

Australia

Purpose for transfer and any further processing	**Internal transfer**: Jamf has an office in Australia, and employees there may need to process the customer's personal data for the purposes of support, security, or cloud hosting. **Transfer to sub-processor**: Jamf Pro and Protect uses AWS to store data in Australia.

	Jamf uses AWS to process data in Australia as part of Jamf Data Policy, Private Access, Threat Defense, and Safe Internet edge services if the customer chooses this location. Data is then transferred to Ireland for storage and further processing. Please see our list of sub-processors for specific information.
The frequency of the transfer	**Internal transfer**: Data is transferred as needed to provide support and hosted services. **Transfer to sub-processor**: Data is transferred continuously to AWS for customers that choose this region for hosting.
Categories of personal data transferred	See Section B of Schedule 1 to Jamf's DPA.
Sensitive data transferred	None
Applied restrictions or safeguards that take into consideration the nature of the data and the risks involved	**Internal transfer**: Jamf's security measures for internal transfers are set forth in Schedule 3 of Jamf's DPA and on Jamf's Security Portal. **Transfer to sub-processor**: Jamf enters into appropriate data processing agreements with all sub-processors that include data protection obligations that offer at least the same protection of personal data that Jamf offers to its customers.
Supplemental Organizational, Technical, and Contractual Security Measures	**Internal transfer**: Jamf's security measures for internal transfers are set forth in Schedule 3 of Jamf's DPA and on Jamf's Security Portal.

	Transfer to sub-processor: Jamf enters into appropriate data processing agreements with all sub-processors that include data protection obligations that offer at least the same protection of personal data that Jamf offers to its customers. Sub-processors have been verified by Jamf's Information Security team to have sufficient technical and organizational security measures.
Jamf Policy for Law Enforcement Requests to Client Data	**Internal Transfer:** Jamf's DPA compels us to notify our customer of requests unless explicitly prohibited from doing so by law. Please note that Jamf does not and cannot conduct real-time surveillance of customers. To date, Jamf has not received a request from law enforcement for client data. **Transfer to sub-processor**: Jamf ensures that the data processing agreements with its sub-processors have appropriate obligations with respect to law enforcement requests to enable Jamf to comply with Jamf's obligations to customers under our DPA.
Length of processing chain	**Internal transfer:** Data is transferred internally within Jamf. **Transfer to sub-processor**: Data is transferred externally to our sub-processors.
Applicable transfer mechanism	**Internal transfer**: EEA SCCs and the UK Addendum (as applicable) incorporated into Jamf's DPA. **Transfer to sub-processor**: EEA SCCs and the UK Addendum (as applicable) for onward transfers to our sub-processors.

Brazil

Purpose for transfer and any further processing	**Transfer to sub-processor**: Jamf uses AWS to process data in Brazil as part of Jamf Data Policy, Private Access, Threat Defense, Safe Internet edge services if the customer chooses this location. Data is then transferred to Ireland for storage and further processing. Please see our list of sub-processors for specific information.
The frequency of the transfer	**Transfer to sub-processor**: Data is transferred continuously to AWS for customers that choose this region for their edge.
Categories of personal data transferred	See Section B of Schedule 1 to Jamf's DPA.
Sensitive data transferred	None
Applied restrictions or safeguards that take into consideration the nature of the data and the risks involved	**Transfer to sub-processor**: Jamf enters into appropriate data processing agreements with all sub-processors that include data protection obligations that offer at least the same protection of personal data that Jamf offers to its customers.
Supplemental Organizational, Technical, and Contractual Security Measures	**Transfer to sub-processor**: Jamf enters into appropriate data processing agreements with all sub-processors that include data protection obligations that offer at least the same protection of personal data that Jamf offers to its customers. Sub-processors have been verified by Jamf's Information Security team to have sufficient technical and

	organizational security measures.
Jamf Policy for Law Enforcement Requests to Client Data	**Transfer to sub-processor**: Jamf ensures that the data processing agreements with its sub-processors have appropriate obligations with respect to law enforcement requests to enable Jamf to comply with Jamf's obligations to customers under our DPA.
Length of processing chain	**Transfer to sub-processor**: Data is transferred externally to our sub-processors.
Applicable transfer mechanism	**Transfer to sub-processor**: EEA SCCs and the UK Addendum (as applicable) for onward transfers to our sub-processors.

Canada

Purpose for transfer and any further processing	**Transfer to sub-processor**: Jamf uses AWS and IBM Softlayer to process data in Canada as part of Jamf Data Policy, Private Access, Threat Defense, and Safe Internet edge services if the customer chooses this location. Data is then transferred to Ireland for storage and further processing. Please see our list of sub-processors for specific information.
The frequency of the transfer	**Transfer to sub-processor**: Data is transferred continuously to AWS and IBM Softlayer for customers that choose this region for their edge.
Categories of personal data transferred	See Section B of Schedule 1 to Jamf's DPA.
Sensitive data transferred	None

Applied restrictions or safeguards that take into consideration the nature of the data and the risks involved	**Transfer to sub-processor**: Jamf enters into appropriate data processing agreements with all sub-processors that include data protection obligations that offer at least the same protection of personal data that Jamf offers to its customers.
Supplemental Organizational, Technical, and Contractual Security Measures	**Transfer to sub-processor**: Jamf enters into appropriate data processing agreements with all sub-processors that include data protection obligations that offer at least the same protection of personal data that Jamf offers to its customers. Sub-processors have been verified by Jamf's Information Security team to have sufficient technical and organizational security measures.
Jamf Policy for Law Enforcement Requests to Client Data	**Transfer to sub-processor**: Jamf ensures that the data processing agreements with its sub-processors have appropriate obligations with respect to law enforcement requests to enable Jamf to comply with Jamf's obligations to customers under our DPA.
Length of processing chain	**Transfer to sub-processor**: Data is transferred externally to our sub-processors.
Applicable transfer mechanism	**Transfer to sub-processor**: EEA SCCs and the UK Addendum (as applicable) for onward transfers to our sub-processors.

Hong Kong

Purpose for transfer and any further processing	**Transfer to sub-processor**: Jamf uses AWS and IBM Softlayer to process data in Hong Kong as part of Jamf Data Policy, Threat Defense, and Safe Internet edge services if the customer chooses this location. Data is

	then transferred to Ireland for storage and further processing. Please see our list of sub-processors for specific information.
The frequency of the transfer	**Transfer to sub-processor**: Data is transferred continuously to AWS and IBM Softlayer for customers that choose this region for their edge.
Categories of personal data transferred	See Section B of Schedule 1 to Jamf's DPA.
Sensitive data transferred	None
Applied restrictions or safeguards that take into consideration the nature of the data and the risks involved	**Transfer to sub-processor**: Jamf enters into appropriate data processing agreements with all sub-processors that include data protection obligations that offer at least the same protection of personal data that Jamf offers to its customers.
Supplemental Organizational, Technical, and Contractual Security Measures	**Transfer to sub-processor**: Jamf enters into appropriate data processing agreements with all sub-processors that include data protection obligations that offer at least the same protection of personal data that Jamf offers to its customers. Sub-processors have been verified by Jamf's Information Security team to have sufficient technical and organizational security measures.
Jamf Policy for Law Enforcement Requests to Client Data	**Transfer to sub-processor**: Jamf ensures that the data processing agreements with its sub-processors have appropriate obligations with respect to law enforcement requests to enable Jamf to comply with Jamf's obligations to customers under our DPA.

Length of processing chain	**Transfer to sub-processor**: Data is transferred externally to our sub-processors.
Applicable transfer mechanism	**Transfer to sub-processor**: EEA SCCs and the UK Addendum (as applicable) for onward transfers to our sub-processors.

India

Purpose for transfer and any further processing	**Transfer to sub-processor**: Jamf uses AWS to process data in India as part of Jamf Data Policy, Private Access, Threat Defense, and Safe Internet edge services if the customer chooses this location. Data is then transferred to Ireland for storage and further processing. Please see our list of sub-processors for specific information.
The frequency of the transfer	**Transfer to sub-processor**: Data is transferred continuously to AWS for customers that choose this region for their edge.
Categories of personal data transferred	See Section B of Schedule 1 to Jamf's DPA.
Sensitive data transferred	None
Applied restrictions or safeguards that take into consideration the nature of the data and the risks involved	**Transfer to sub-processor**: Jamf enters into appropriate data processing agreements with all sub-processors that include data protection obligations that offer at least the same protection of personal data that Jamf offers to its customers.
Supplemental Organizational, Technical, and Contractual Security Measures	**Transfer to sub-processor**: Jamf enters into appropriate data processing agreements with all sub-processors that include data

	protection obligations that offer at least the same protection of personal data that Jamf offers to its customers. Sub-processors have been verified by Jamf's Information Security team to have sufficient technical and organizational security measures.
Jamf Policy for Law Enforcement Requests to Client Data	**Transfer to sub-processor**: Jamf ensures that the data processing agreements with its sub-processors have appropriate obligations with respect to law enforcement requests to enable Jamf to comply with Jamf's obligations to customers under our DPA.
Length of processing chain	**Transfer to sub-processor**: Data is transferred externally to our sub-processors.
Applicable transfer mechanism	**Transfer to sub-processor**: EEA SCCs and the UK Addendum (as applicable) for onward transfers to our sub-processors.

Japan

Purpose for transfer and any further processing	**Internal transfer**: Jamf has an office in Japan, and employees there may need to process customer personal data for the purposes of support, security, or cloud hosting. **Transfer to sub-processor**: Jamf Pro, Protect, and School each use AWS to store data in Japan. Jamf uses AWS and IBM Softlayer to process data in Japan as part of Jamf Data Policy, Private Access, Threat Defense, and Safe Internet edge services if the customer chooses this location. Data is then

	transferred to Ireland for storage and further processing. Please see our list of sub-processors for specific information.
The frequency of the transfer	**Internal transfer**: Data is transferred as needed to provide support and hosted services. **Transfer to sub-processor**: Data is transferred continuously to AWS for customers that choose this region for hosting.
Categories of personal data transferred	See Section B of Schedule 1 of Jamf's DPA.
Sensitive data transferred	None
Applied restrictions or safeguards that take into consideration the nature of the data and the risks involved	**Internal transfer**: Jamf's security measures for internal transfers are set forth in Schedule 3 of Jamf's DPA and on Jamf's Security Portal. **Transfer to sub-processor**: Jamf enters into appropriate data processing agreements with all sub-processors that include data protection obligations that offer at least the same protection of personal data that Jamf offers to its customers.
Supplemental Organizational, Technical, and Contractual Security Measures	**Internal transfer**: Jamf's security measures for internal transfers are set forth in Schedule 3 of Jamf's DPA and on Jamf's Security Portal. **Transfer to sub-processor**: Jamf enters into appropriate data processing agreements with all sub-processors that include data protection obligations that offer at least the

	same protection of personal data that Jamf offers to its customers. Sub-processors have been verified by Jamf's Information Security team to have sufficient technical and organizational security measures.
Jamf Policy for Law Enforcement Requests to Client Data	**Internal Transfer:** Jamf's DPA compels us to notify our customer of requests unless explicitly prohibited from doing so by law. Please note that Jamf does not and cannot conduct real-time surveillance of customers. To date, Jamf has not received a request from law enforcement for client data. **Transfer to sub-processor**: Jamf ensures that the data processing agreements with its sub-processors have appropriate obligations with respect to law enforcement requests to enable Jamf to comply with Jamf's obligations to customers under our DPA.
Length of processing chain	**Internal transfer:** Data is transferred internally within Jamf. **Transfer to sub-processor**: Data is transferred externally to our sub-processor.
Applicable transfer mechanism	**Internal transfer**: EEA SCCs and the UK Addendum (as applicable) incorporate into Jamf's DPA. **Transfer to sub-processor**: EEA SCCs or the UK Addendum (as applicable) for onward transfers to our sub-processors.

Mexico

Purpose for transfer and any further processing	**Transfer to sub-processor**: Jamf uses IBM Softlayer to process data in Mexico as part of Jamf Data Policy, Threat Defense, and Safe Internet edge services if the customer chooses this location. Data is then transferred to Ireland for storage and further processing. Please see our list of sub-processors for specific information.
The frequency of the transfer	**Transfer to sub-processor**: Data is transferred continuously to IBM Softlayer for customers that choose this region for their edge.
Categories of personal data transferred	See Section B of Schedule 1 to Jamf's DPA.
Sensitive data transferred	None
Applied restrictions or safeguards that take into consideration the nature of the data and the risks involved	**Transfer to sub-processor**: Jamf enters into appropriate data processing agreements with all sub-processors that include data protection obligations that offer at least the same protection of personal data that Jamf offers to its customers.
Supplemental Organizational, Technical, and Contractual Security Measures	**Transfer to sub-processor**: Jamf enters into appropriate data processing agreements with all sub-processors that include data protection obligations that offer at least the same protection of personal data that Jamf offers to its customers. Sub-processors have been verified by Jamf's Information Security team to have sufficient technical and

	organizational security measures.
Jamf Policy for Law Enforcement Requests to Client Data	**Transfer to sub-processor**: Jamf ensures that the data processing agreements with its sub-processors have appropriate obligations with respect to law enforcement requests to enable Jamf to comply with Jamf's obligations to customers under our DPA.
Length of processing chain	**Transfer to sub-processor**: Data is transferred externally to our sub-processors.
Applicable transfer mechanism	**Transfer to sub-processor**: EEA SCCs and the UK Addendum (as applicable) for onward transfers to our sub-processors.

Singapore

Purpose for transfer and any further processing	**Transfer to sub-processor**: Jamf uses AWS and IBM Softlayer to process data in Singapore as part of Jamf Data Policy, Threat, Private Access, Threat Defense, and Safe Internet edge services if the customer chooses this location. Data is then transferred to Ireland for storage and further processing. Please see our list of sub-processors for specific information.
The frequency of the transfer	**Transfer to sub-processor**: Data is transferred continuously to AWS and IBM Softlayer for customers that choose this region for their edge.
Categories of personal data transferred	See Section B of Schedule 1 to Jamf's DPA.
Sensitive data transferred	None

Applied restrictions or safeguards that take into consideration the nature of the data and the risks involved	**Transfer to sub-processor**: Jamf enters into appropriate data processing agreements with all sub-processors that include data protection obligations that offer at least the same protection of personal data that Jamf offers to its customers.
Supplemental Organizational, Technical, and Contractual Security Measures	**Transfer to sub-processor**: Jamf enters into appropriate data processing agreements with all sub-processors that include data protection obligations that offer at least the same protection of personal data that Jamf offers to its customers. Sub-processors have been verified by Jamf's Information Security team to have sufficient technical and organizational security measures.
Jamf Policy for Law Enforcement Requests to Client Data	**Transfer to sub-processor**: Jamf ensures that the data processing agreements with its sub-processors have appropriate obligations with respect to law enforcement requests to enable Jamf to comply with Jamf's obligations to customers under our DPA.
Length of processing chain	**Transfer to sub-processor**: Data is transferred externally to our sub-processors.
Applicable transfer mechanism	**Transfer to sub-processor**: EEA SCCs and the UK Addendum (as applicable) for onward transfers to our sub-processors.

South Africa

Purpose for transfer and any further processing	**Transfer to sub-processor**: Jamf uses AWS to process data in South Africa as part of Jamf Data Policy, Private Access, Threat Defense, and Safe Internet edge services if the customer chooses this location. Data is then transferred to Ireland for storage and further processing. Please see our list of sub-processors for specific information.
The frequency of the transfer	**Transfer to sub-processor**: Data is transferred continuously to AWS for customers that choose this region for their edge.
Categories of personal data transferred	See Section B of Schedule 1 to Jamf's DPA.
Sensitive data transferred	None
Applied restrictions or safeguards that take into consideration the nature of the data and the risks involved	**Transfer to sub-processor**: Jamf enters into appropriate data processing agreements with all sub-processors that include data protection obligations that offer at least the same protection of personal data that Jamf offers to its customers.
Supplemental Organizational, Technical, and Contractual Security Measures	**Transfer to sub-processor**: Jamf enters into appropriate data processing agreements with all sub-processors that include data protection obligations that offer at least the same protection of personal data that Jamf offers to its customers. Sub-processors have been verified by Jamf's Information Security team to have sufficient technical and

	organizational security measures.
Jamf Policy for Law Enforcement Requests to Client Data	**Transfer to sub-processor**: Jamf ensures that the data processing agreements with its sub-processors have appropriate obligations with respect to law enforcement requests to enable Jamf to comply with Jamf's obligations to customers under our DPA.
Length of processing chain	**Transfer to sub-processor**: Data is transferred externally to our sub-processors.
Applicable transfer mechanism	**Transfer to sub-processor**: EEA SCCs and the UK Addendum (as applicable) for onward transfers to our sub-processors.

South Korea

Purpose for transfer and any further processing	**Transfer to sub-processor**: Jamf uses AWS and IBM Softlayer to process data in South Korea as part of Jamf Data Policy, Threat Defense, and Safe Internet edge services if the customer chooses this location. Data is then transferred to Ireland for storage and further processing. Please see our list of sub-processors for specific information.
The frequency of the transfer	**Transfer to sub-processor**: Data is transferred continuously to AWS and IBM Softlayer for customers that choose this region for their edge.

Categories of personal data transferred	See Section B of Schedule 1 to Jamf's DPA.
Sensitive data transferred	None
Applied restrictions or safeguards that take into consideration the nature of the data and the risks involved	**Transfer to sub-processor**: Jamf enters into appropriate data processing agreements with all sub-processors that include data protection obligations that offer at least the same protection of personal data that Jamf offers to its customers.
Supplemental Organizational, Technical, and Contractual Security Measures	**Transfer to sub-processor**: Jamf enters into appropriate data processing agreements with all sub-processors that include data protection obligations that offer at least the same protection of personal data that Jamf offers to its customers. Sub-processors have been verified by Jamf's Information Security team to have sufficient technical and organizational security measures.
Jamf Policy for Law Enforcement Requests to Client Data	**Transfer to sub-processor**: Jamf ensures that the data processing agreements with its sub-processors have appropriate obligations with respect to law enforcement requests to enable Jamf to comply with Jamf's obligations to customers under our DPA.
Length of processing chain	**Transfer to sub-processor**: Data is transferred externally to our sub-processors.
Applicable transfer mechanism	**Transfer to sub-processor**: EEA SCCs and the UK Addendum (as applicable) for onward transfers to our sub-processors.

Switzerland

Purpose for transfer and any further processing	**Transfer to sub-processor**: Jamf uses Microsoft Azure to process data in Switzerland as part of Jamf Data Policy, Threat Defense, and Safe Internet edge services if the customer chooses this location. Data is then transferred to Ireland for storage and further processing. Please see our list of sub-processors for specific information.
The frequency of the transfer	**Transfer to sub-processor**: Data is transferred continuously to Microsoft Azure for customers that choose this region for their edge.
Categories of personal data transferred	See Section B of Schedule 1 to Jamf's DPA.
Sensitive data transferred	None
Applied restrictions or safeguards that take into consideration the nature of the data and the risks involved	**Transfer to sub-processor**: Jamf enters into appropriate data processing agreements with all sub-processors that include data protection obligations that offer at least the same protection of personal data that Jamf offers to its customers.
Supplemental Organizational, Technical, and Contractual Security Measures	**Transfer to sub-processor**: Jamf enters into appropriate data processing agreements with all sub-processors that include data protection obligations that offer at least the same protection of personal data that Jamf offers to its customers. Sub-processors have been verified by Jamf's Information Security team to have sufficient technical and organizational security measures.

Jamf Policy for Law Enforcement Requests to Client Data	**Transfer to sub-processor**: Jamf ensures that the data processing agreements with its sub-processors have appropriate obligations with respect to law enforcement requests to enable Jamf to comply with Jamf's obligations to customers under our DPA.
Length of processing chain	**Transfer to sub-processor**: Data is transferred externally to our sub-processors.
Applicable transfer mechanism	**Transfer to sub-processor**: EEA SCCs and the UK Addendum (as applicable) for onward transfers to our sub-processors.

United Kingdom

Purpose for transfer and any further processing	**Internal transfer**: Jamf has an office in the United Kingdom, and employees there may need to process customer personal data for the purposes of support, security, or cloud hosting. **Transfer to sub-processor**: Jamf Pro and Protect uses AWS to store data in the United Kingdom. Jamf uses AWS, IBM Softlayer, and Rackspace to process data in the United Kingdom as part of Jamf Data Policy, Private Access, Threat Defense, and Safe Internet edge services if customers choose this location. Please see our list of sub-processors for specific information.

The frequency of the transfer	**Internal transfer**: Data is transferred as needed to provide support and hosted services. **Transfer to sub-processor**: Data is transferred continuously to AWS, IBM Softlayer, and Rackspace for customers that choose this region for hosting.
Categories of personal data transferred	See Section B of Schedule 1 to Jamf's DPA.
Sensitive data transferred	None
Applied restrictions or safeguards that take into consideration the nature of the data and the risks involved	**Internal transfer**: Jamf's security measures for internal transfers are set forth in Schedule 3 of Jamf's DPA and on Jamf's Security Portal. **Transfer to sub-processor**: Jamf enters into appropriate data processing agreements with all sub-processors that include data protection obligations that offer at least the same protection of personal data that Jamf offers to its customers.
Supplemental Organizational, Technical, and Contractual Security Measures	**Internal transfer**: Jamf's security measures for internal transfers are set forth in Schedule 3 of Jamf's DPA and on Jamf's Security Portal. **Transfer to sub-processor**: Jamf enters into appropriate data processing agreements with all sub-processors that include data protection obligations that offer at least the same protection of personal data that Jamf offers to its customers. Sub-processors have been verified by Jamf's Information Security team to have sufficient technical and organizational security measures.
Jamf Policy for Law Enforcement Requests to Client Data	**Internal Transfer:** Jamf's DPA compels us to notify our customer of requests unless

	explicitly prohibited from doing so by law. Please note that Jamf does not and cannot conduct real-time surveillance of customers. To date, Jamf has not received a request from law enforcement for client data. **Transfer to sub-processor**: Jamf ensures that the data processing agreements with its sub-processors have appropriate obligations with respect to law enforcement requests to enable Jamf to comply with Jamf's obligations to customers under our DPA.
Length of processing chain	**Internal transfer:** Data is transferred internally within Jamf. **Transfer to sub-processor**: Data is transferred externally to our sub-processor.
Applicable transfer mechanism	**Internal transfer**: EEA SCCs and the UK Addendum to them are incorporated into Jamf's DPA. **Transfer to sub-processor**: EEA SCCs and the UK Addendum to them for onward transfer to our sub-processor.

United States

Purpose for transfer and any further processing	**Internal transfer**: Jamf's headquarters and many offices are located in the United States, and employees there may need to process customer personal data for the purposes of support, security, or cloud hosting.

	Transfer to sub-processor: Jamf Connect, Now, Pro, Protect, and School uses AWS to store data in the United States. Jamf uses AWS, IBM Softlayer, and Rackspace to process data in the United States as part of Jamf Data Policy, Private Access, Threat Defense, and Safe Internet edge services if the customer chooses this location. Data is then transferred to Ireland for storage and further processing. Jamf uses Mailchimp and Twilio at a customer's choosing for email notifications. Please see our list of sub-processors for specific information.
The frequency of the transfer	**Internal transfer**: Data is transferred as needed to provide support and hosted services. **Transfer to sub-processor**: Data is transferred continuously to AWS, IBM Softlayer, and Rackspace for customers that choose this region for hosting.
Categories of personal data transferred	See Section B of Schedule 1 in Jamf's DPA.
Sensitive data transferred	None.
Applied restrictions or safeguards that take into consideration the nature of the data and the risks involved	**Internal transfer**: Jamf's security measures for internal transfers are set forth in Schedule 3 of Jamf's DPA and on Jamf's Security Portal. **Transfer to sub-processor**: Jamf enters into appropriate data processing agreements with all sub-processors that include data protection obligations that offer at least the same protection of personal data that Jamf

	offers its customers.
Supplemental Organizational, Technical, and Contractual Security Measures	**Internal transfer**: Jamf's security measures for internal transfers are set forth in Schedule 3 of Jamf's DPA and on Jamf's Security Portal. **Transfer to sub-processor**: Jamf enters into appropriate data processing agreements with all sub-processors that include data protection obligations that offer at least the same protection of personal data that Jamf offers to its customers. Sub-processors have been verified by Jamf's Information Security team to have sufficient technical and organizational security measures.

Jamf Policy for Law Enforcement Requests to Client Data	**Internal Transfer:** Jamf's DPA compels us to notify our customer of requests unless explicitly prohibited from doing so by law. Please note that Jamf does not and cannot conduct real-time surveillance of customers. To date, Jamf has not received a request from law enforcement for client data. **Transfer to sub-processor**: Jamf ensures that the data processing agreements with its sub-processors have appropriate obligations with respect to law enforcement requests to enable Jamf to comply with Jamf's obligations to customers under our DPA.
Length of processing chain	**Internal transfer:** Data is transferred internally within Jamf. **Transfer to sub-processor**: Data is transferred externally to our sub-processor.
Applicable transfer mechanism	**Internal transfer**: To the extent applicable, the EEA SCCs and the UK Addendum, which are incorporate into Jamf's DPA. **Transfer to sub-processor**: To the extent applicable, the EEA SCCs and the UK Addendum for onward transfers to our sub-processors.

Last Updated: September 20, 2022