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"),UK Addendum, or the EEA SCCs subject to modifications and amendments prescribed by the Swiss Federal Data Protection and Information Commissioner ("Swiss SCCs").

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, UK Addendum, and Swiss 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.

Jamf relies on our DPA as the transfer mechanism used to transfer personal data outside the EEA, UK and/or Switzerland. Jamf's DPA incorporates the EEA SCCs, UK Addendum, and Swiss SCCs. In addition, Jamf is certified as a participant in the EU-U.S. and Swiss-U.S. Data Privacy Frameworks, as well as the UK Extension to the EU-U.S. Data Privacy Framework. You can confirm Jamf's participation here: Data Privacy Framework Participant Search.

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.

Certain Jamf products do not allow for regional data hosting. For Jamf Manager for Android and Jamf Now, all data is hosted in the United States. Jamf Pro, Jamf Safe Internet, and Jamf School allow for regional data hosting. In the case of Jamf Data Policy, Jamf Executive Threat Protection, Jamf Private Access, and Jamf Threat Defense, data is only hosted in Ireland. Jamf Protect and Jamf Connect allow for regional data hosted with the exception of certain functionality, in which case data is hosted in Ireland.

Please refer to Jamf's Sub-processors documentation to better understand where your data may be stored for each product or service you subscribe to.

US Surveillance Laws

Is Jamf subject to FISA 702, EO 12333 or the CLOUD Act?

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.

Where Jamf is deemed to be a RCSP, the CLOUD Act could apply to Jamf. However, we don't believe the type of data processed on behalf of Jamf customers would be of interest to the U.S. Government or law enforcement authorities. The CLOUD Act does not make data easily accessible to the U.S. Government. It operates, in part to amend the Electronic Communications Privacy Act, which is a law that prescribes how law enforcement agencies may obtain information from technology companies. These laws address access to electronic data in relation to government efforts to protect public safety and combat serious crime, as well as to address conflicting laws between the U.S. and other countries by creating a framework for the U.S. Government to resolve conflicts and mutually agree to respect law and privacy.

Under the CLOUD Act, electronic content can only be requested from providers with a warrant that must identify the data being sought. The warrant must be approved by a court, and if approved, the CLOUD Act allows providers, like Jamf, to challenge the court order, particularly if there are conflicts with a foreign country's laws. Jamf will take reasonably necessary actions if served with a warrant related to a CLOUD Act data request to protect data in its possession, including ensuring compliance with Section 4 g) of Jamf's DPA. The CLOUD Act does not allow the U.S. Government to collect bulk data – the data requested must be specific and the warrant needs to be based on probable cause for a crime.

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 the CLOUD Act 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

Jamf provides hosting locations that may differ between products and features within certain products. Please review the locations of data hosting for the products and services you subscribe to in our Sub-processors documentation.

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 or hosting services. **Transfer to sub-processor**: Jamf Pro and Protect uses AWS to store data in Australia. Jamf uses AWS for our edge services to process data in Australia as part of Jamf Data Policy, Now, Private Access, Safe Internet, and Threat Defense. Jamf Connect and Protect include features that may also use these edge services. Data related to these products and features is then transferred to Ireland or the United States (hosting option for Jamf Safe Internet only) for storage and

	further processing. Jamf Now is hosted on AWS exclusively in the United States. 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 hosting services. **Transfer to sub-processor**: Data is transferred continuously to AWS for customers in this region for hosting and edge services.
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, UK Addendum, and/or Swiss SCCs (as applicable), which are incorporated into Jamf's DPA. **Transfer to sub-processor**: EEA SCCs, UK Addendum, and/or Swiss SCCs (as applicable) for onward transfers to our sub-processors.

Belgium

Purpose for transfer and any further processing	**Transfer to sub-processor**: Jamf uses Google Cloud Platform for our edge

	services to process data in Belgium as part of Jamf Data Policy, Safe Internet, and Threat Defense, Jamf Protect includes features that may also use these edge services. Data related to these products and features is then transferred to Ireland or the United States (hosting option for Jamf Safe Internet only) 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 Google Cloud Platform for customers in this region for their edge services.
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, UK Addendum, and/or Swiss SCCs (as applicable) for onward transfers to our sub-processors.

Brazil

Purpose for transfer and any further processing	**Transfer to sub-processor**: Jamf uses AWS for our edge services to process data in Brazil as part of Jamf Data Policy, Now, Private Access, Safe Internet, and Threat Defense. Jamf Connect and Protect include features that may also use these edge services. Data related to these products and features is then transferred to Ireland or the United States (hosting option for Jamf Safe Internet only) for storage and further processing. Jamf Now is hosted on AWS exclusively in the United States. 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 in this region for their edge services.
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, UK Addendum, and/or Swiss SCCs (as applicable) for onward transfers to our sub-processors.

Canada

Purpose for transfer and any further processing	**Transfer to sub-processor**: Jamf uses AWS for our edge services to process data in Canada as part of Jamf Data Policy, Now, Private Access, Safe Internet, and Threat Defense. Jamf

	Connect and Protect include features that may also use these edge services. Data related to these products and features is then transferred to Ireland or the United States (hosting option for Jamf Safe Internet only) for storage and further processing. Jamf Now is hosted on AWS exclusively in the United States. 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 in this region for their edge services.
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, UK Addendum, and/or Swiss SCCs (as applicable) for onward transfers to our sub-processors.

Czechia

Purpose for transfer and any further processing	**Internal transfer**: Jamf has an office in Czechia, and employees there may need to process the customer's personal data for the purposes of security operations.
The frequency of the transfer	**Internal transfer**: Data is transferred as needed for security operations.
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.
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.
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.
Length of processing chain	**Internal transfer:** Data is transferred internally within Jamf.
Applicable transfer mechanism	**Internal transfer**: EEA SCCs, UK Addendum, and/or Swiss SCCs (as applicable), which are incorporated into Jamf's DPA.

France

Purpose for transfer and any further processing	**Internal transfer**: Jamf has an office in France, and employees there may need to process the customer's personal data for the purposes of support. **Transfer to sub-processor**: Jamf uses AWS for our edge services to process data in France as part of Jamf Data Policy, Now, Safe Internet, and Threat Defense. Jamf Protect includes features that may also use these edge services. Data related to these products and features is then transferred to Ireland or the United States (hosting option for Jamf Safe Internet only) for storage and further processing. Jamf Now is hosted on AWS exclusively in the United States. 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.

	Transfer to sub-processor: Data is transferred continuously to AWS for customers in this region for their edge services.
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, UK Addendum, and/or Swiss SCCs (as applicable), which are incorporated into Jamf's DPA. **Transfer to sub-processor**: EEA SCCs, UK Addendum, and/or Swiss SCCs (as applicable) for onward transfers to our sub-processors.

Germany

Purpose for transfer and any further processing	**Internal transfer**: Jamf has an office in Germany, and employees there may need to process the customer's personal data for the purposes of support. **Transfer to sub-processor**: Jamf Pro, Protect, and School uses AWS to store data in Germany. Jamf Pro may use Microsoft Corporation to host data in Germany for customers purchasing through the MS Azure Marketplace.

	Jamf uses AWS for our edge services to process data in Germany as part of Jamf Data Policy, Now, Private Access, Safe Internet, and Threat Defense. Jamf Connect and Protect include features that may also use these edge services. Data related to these products and features is then transferred to Ireland or the United States (hosting option for Jamf Safe Internet only) for storage and further processing. Jamf uses T-Systems International GmbH for our edge services to process data in Germany as part of Jamf Data Policy and Threat Defense. Jamf Protect includes features that may also use these edge services. Data related to these products and features are then transferred to Ireland for storage and further processing. Jamf uses Deutsche Telekom for our edge services to process data in Germany as part of Jamf Data Policy and Threat Defense for Deutsche Telekom customers only. Jamf Protect includes features that may also use these edge services for Deutsche Telekom customers only. Data for these products and features 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. **Transfer to sub-processor**: Data is transferred continuously to AWS for customers in this region for hosting and edge services.

	Data is transferred continuously to Deutsche Telekom for Deutsche Telekom customers in this region for edge services.
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, UK Addendum, and/or Swiss SCCs (as applicable), which are incorporated into Jamf's DPA. **Transfer to sub-processor**: EEA SCCs, UK Addendum, and/or Swiss SCCs (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 for our edge services to process data in Hong Kong as part of Jamf Data Policy, Private Access, Safe Internet, and Threat Defense. Jamf Connect and Protect include features that may also use these edge services. Data related to these products and features is then transferred to Ireland or the United States (hosting option for Jamf Safe Internet only) 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 in this region for their edge service.
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, UK Addendum, and/or Swiss SCCs (as applicable) for onward transfers to our sub-processors.

India

Purpose for transfer and any further processing	**Internal transfer**: Jamf has an office in India, and employees there may need to process the customer's personal data for the purpose of support. **Transfer to sub-processor**: Jamf uses AWS for our edge services to process data in India as part of Jamf Data Policy, Now, Private Access, Safe Internet, and Threat Defense. Jamf Connect and Protect include features that may also use these edge services. Data related to these products and features is then transferred to Ireland or the United States (hosting option for Jamf Safe Internet only) for storage and further processing. Jamf Now is hosted on AWS exclusively in the United States. Please see our list of sub-processors for specific information.
The frequency of the transfer	**Internal transfer:** Data is transferred to provide support. **Transfer to sub-processor**: Data is transferred continuously to AWS for customers in this region for their edge service.
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, UK Addendum, and/or Swiss SCCs (as applicable), which are incorporated into Jamf's DPA. **Transfer to sub-processor**: EEA SCCs, UK Addendum, and/or Swiss SCCs (as applicable) for onward transfers to our sub-processors.

Ireland

Purpose for transfer and any further processing	**Transfer to sub-processor**: Jamf Data Policy, Executive Threat Protection, Private Access, Safe Internet, and Threat Defense utilize AWS for data storage in Ireland. Select features within Jamf Connect and Protect may also store data in Ireland. Jamf uses AWS for our edge services to process data in Ireland as part of Jamf Data Policy, Now, Private Access, Safe Internet, and Threat Defense. Select features in Jamf Connect and Protect may also process data through our edge services in Ireland. For Jamf Safe Internet, data may be transferred to the United States for hosting and additional processing if chosen by the customer. Jamf Now is hosted on AWS exclusively in the United States.

	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 in this region for their edge services.
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	**Internal transfer**: EEA SCCs, UK Addendum, and/or Swiss SCCs (as applicable), which are incorporated into Jamf's DPA.

Israel

Purpose for transfer and any further processing	**Internal transfer**: Jamf has an office in Israel, and employees there may need to process customer's personal data for the purposes of support.
The frequency of the transfer	**Internal transfer**: Data is transferred as needed for support.
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.
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.
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.

Length of processing chain	**Internal transfer:** Data is transferred internally within Jamf.
Applicable transfer mechanism	**Internal transfer**: EEA SCCs, UK Addendum, and/or Swiss SCCs (as applicable), which are incorporated into Jamf's DPA.

Italy

Purpose for transfer and any further processing	**Transfer to sub-processor**: Jamf uses AWS for our edge services to process data in Italy as part of Jamf Data Policy, Now, Safe Internet, and Threat Defense. Jamf Protect includes features that may also use these edge services. Data related to these products and features is then transferred to Ireland or the United States (hosting option for Jamf Safe Internet only) for storage and further processing. Jamf Now is hosted on AWS exclusively in the United States. 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 in this region for their edge services.
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, UK Addendum, and/or Swiss SCCs (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 or cloud hosting. **Transfer to sub-processor**: Jamf Pro, Protect, and School each use AWS to store data in Japan.

	Jamf uses AWS for our edge services to process data in Japan as part of Jamf Data Policy, Now, Private Access, Safe Internet, and Threat Defense. Jamf Connect and Protect include features that may also use these edge services. Data related to these products and features is then transferred to Ireland or the United States (hosting option for Jamf Safe Internet only) for storage and further processing. Jamf Now is hosted on AWS exclusively in the United States. 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 hosting services. **Transfer to sub-processor**: Data is transferred continuously to AWS for customers in this region for hosting and edge services.
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, UK Addendum, and/or Swiss SCCs (as applicable), which are incorporated into Jamf’s DPA. **Transfer to sub-processor**: EEA SCCs, UK Addendum, and/or Swiss SCCs (as

	applicable) for onward transfers to our sub-processors.

Netherlands

Purpose for transfer and any further processing	**Internal transfer**: Jamf has an office in the Netherlands, and employees there may need to process customer personal data for the purposes of support or cloud hosting. **Transfer to sub-processor**: Jamf uses Google Cloud Platform for our edge services to process data in the Netherlands as part of Jamf Data Policy, Safe Internet, and Threat Defense. Jamf Protect includes features that may also use these edge services. Data related to these products and features is then transferred to Ireland or the United States (hosting option for Jamf Safe Internet only) 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 hosting services. **Transfer to sub-processor**: Data is transferred continuously to Google Cloud Platform for customers in this region for their edge services.
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, UK Addendum, and/or Swiss SCCs (as applicable), which are incorporated into Jamf's DPA. **Transfer to sub-processor**: EEA SCCs, UK Addendum, and/or Swiss SCCs (as applicable) for onward transfers to our sub-processors.

Poland

Purpose for transfer and any further processing	**Internal transfer**: Jamf has an office in Poland, and employees there may need to process the customer's personal data for the purposes of support, security operations, or hosting services.
The frequency of the transfer	**Internal transfer**: Data is transferred as needed for security support, security operations, or hosting services.
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.
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.
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.
Length of processing chain	**Internal transfer:** Data is transferred internally within Jamf.
Applicable transfer mechanism	**Internal transfer**: EEA SCCs, UK Addendum, and/or Swiss SCCs (as applicable), which are incorporated into Jamf's DPA.

Singapore

Purpose for transfer and any further processing	**Transfer to sub-processor**: Jamf uses AWS for our edge services to process data in Singapore as part of Jamf Data Policy, Now, Private Access, Safe Internet, and Threat Defense. Jamf Connect and Protect include features that may also use these edge services. Data related to these products and features is then transferred to Ireland or the United States (hosting option for Jamf Safe Internet only) for storage and further processing. Jamf Now is hosted on AWS exclusively in the United States. 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 in this region for their edge services.
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, UK Addendum, and/or Swiss SCCs (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 for our edge services to process data in South Africa as part of Jamf Data Policy, Now, Private Access, Safe Internet, and Threat Defense. Jamf Connect and Protect include features that may also use these edge services. Data related to these products and features is then transferred to Ireland or the United States (hosting option for Jamf Safe Internet only) for storage and further processing. Jamf Now is hosted on AWS exclusively in the United States. 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 in this region for their edge services.
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, UK Addendum, and/or Swiss SCCs (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 for our edge services to process data in South Korea as part of Jamf Data Policy, Now, Safe Internet, and Threat Defense. Jamf Protect includes features that may also use these edge services. Data related to these products and features is then transferred to Ireland or the United States (hosting option for Jamf Safe Internet only) for storage and further processing. Jamf Now is hosted on AWS exclusively in the United States. 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 in this region for their edge services.

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, UK Addendum, and/or Swiss SCCs (as applicable) for onward transfers to our sub-processors.

Spain

Purpose for transfer and any further processing	**Transfer to sub-processor**: Jamf uses Google Cloud Platform for our edge

	services to process data in Spain as part of Jamf Data Policy, Safe Internet, and Threat Defense. Jamf Protect includes features that may also use these edge services. Data related to these products and features is then transferred to Ireland or the United States (hosting option for Jamf Safe Internet only) 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 Google Cloud Platform for customers in this region for their edge services.
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, UK Addendum, and/or the Swiss SCCs (as applicable) for onward transfers to our sub-processors.

Sweden

Purpose for transfer and any further processing	**Internal transfer**: Jamf has an office in Sweden, and employees there may need to process customer's personal data for the purposes of support. **Transfer to sub-processor**: Jamf uses AWS for our edge services to process data in Sweden as part of Jamf Data Policy, Now, Safe Internet, and Threat Defense. Jamf Protect includes features that may also use these edge services. Data related to these products and features is then transferred to Ireland or the United States (hosting option for Jamf Safe Internet only) for storage and further processing. Jamf Now is hosted on AWS exclusively in the United States. 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. **Transfer to sub-processor**: Data is transferred continuously to AWS for

	customers in this region for their edge services.
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, UK Addendum and/or Swiss SCCs, which are incorporated into Jamf's DPA. **Transfer to sub-processor**: EEA SCCs, UK Addendum, and/or Swiss SCCs (as applicable) for onward transfers to our sub-processors.

Switzerland

Purpose for transfer and any further processing	**Transfer to sub-processor**: Jamf uses AWS for our edge services to process data in Switzerland as part of Jamf Data Policy, Safe Internet, and Threat Defense. Data related to these products and features is then transferred to Ireland or the United States (hosting option for Jamf Safe Internet only) 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 in this region for their edge services.
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, UK Addendum, and/or Swiss SCCs (as applicable) for onward transfers to our

	sub-processors.

Taiwan

Purpose for transfer and any further processing	**Internal transfer**: Jamf has an office in Taiwan, and employees there may need to process the customer's personal data for the purposes of support or hosting services.
The frequency of the transfer	**Internal transfer**: Data is transferred as needed to provide support or hosting services.
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.
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.
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.

Length of processing chain	**Internal transfer:** Data is transferred internally within Jamf.
Applicable transfer mechanism	**Internal transfer**: EEA SCCs, UK Addendum, and/or Swiss SCCs (as applicable), which are incorporated into Jamf's DPA.

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's personal data for the purposes of support. **Transfer to sub-processor**: Jamf Pro and Protect use AWS to store data in the United Kingdom. Jamf uses AWS for our edge services to process data in the United Kingdom as part of Jamf Data Policy, Now, Private Access, Safe Internet, and Threat Defense. Jamf Connect and Protect include features that may also use these edge services. Data related to these products and features is then transferred to Ireland or the United States (hosting option for Jamf Safe Internet only) for storage and further processing. Jamf Now is hosted on AWS exclusively in the United States. 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. **Transfer to sub-processor**: Data is transferred continuously to AWS for

	customers in this region for hosting or edge services.
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, UK Addendum and/or Swiss SCCs, which are incorporated into Jamf's DPA. **Transfer to sub-processor**: EEA SCCs, UK Addendum and/or Swiss SCCs 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 operations, or hosting services. **Transfer to sub-processor**: Jamf Now, Pro, Protect, Safe Internet, and School use AWS to store data in the United States. Jamf Pro may use Microsoft Corporation to host data in the United States for customers purchasing through the MS Azure Marketplace.

	Jamf Manager for Android uses Google Cloud Platform to store data in the United States. Jamf uses AWS for our edge services to access data in the United States as part of Jamf Data Policy, Now, Private Access, Safe Internet, and Threat Defense. Jamf Connect and Protect include features that may also use these edge services. Data for these products and features is then transferred to Ireland and United States 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, security operations, or hosting services. **Transfer to sub-processor**: Data is transferred continuously to AWS for customers in this region for hosting or edge services.
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, UK Addendum and/or Swiss SCCs, which are incorporated into Jamf's DPA.

	Transfer to sub-processor: To the extent applicable, the EEA SCCs, UK Addendum, and/or Swiss SCCs for onward transfers to our sub-processors.