jamf

To demonstrate how Jamf's ISO certification applies to our compliance with our GDPR obligations, we've provided a mapping of the ISO 27701 controls applicable to our business with the GDPR articles. Should you have further questions, contact **privacy@jamf.com**.

GDPR Articles	Applicable ISO 27701 Controls
Article 5 Principles relating to processing of personal data	6.3.2.1 Mobile device policy 6.5.2.1 Classification of information 6.5.2.2 Labelling of information 6.5.3.1 Management of removable media 6.5.3.2 Disposal of media 6.5.3.3 Physical media transfer 6.6.2.1 User registration and de-registration 6.6.2.2 User access provisioning 6.8.2.7 Secure disposal or re-use of equipment 6.8.2.9 Clear desk and clear screen policy 6.9.3.1 Information backup 6.9.4.1 Event logging 6.6.4.2 Secure log on procedures 6.9.4.2 Protection of log information 6.10.2.1 Information transfer policies and procedures 6.10.2.4 Confidentiality or non-disclosure agreements 6.11.1.2 Securing applications services on public networks 6.11.3.1 Protection of test data 6.12.1.2 Addressing security within supplier agreements 6.13.1.1 Responsibilities and procedures 6.15.1.1 Identification of applicable legislation and contractual requirements 6.15.1.3 Protection of record 7.2.1 Identify and document purpose 7.2.2 Identify lawful basis 7.2.6 Contracts with PII processors 7.2.8 Records related to processing PII 7.3.6 Access, correction and/or erasure 7.4.3 Accuracy and quality 7.4.4 PII minimization objectives 7.4.5 PII de-identification and deletion at the end of processing control 7.4.6 Temporary files control 7.4.8 Disosal 7.4.9 PII transmission controls 8.2.2 Organization's purposes 8.4.1 Temporary files 8.4.3 PII transmission controls

GDPR Articles	Applicable ISO 27701 Controls
Article 6 Lawfulness of processing	7.2.2 Identify lawful basis 7.4.5 PII de-identification and deletion at the end of processing Control
Article 7 Conditions for consent	7.2.4 Obtain and record consent 7.3.4 Providing mechanism to modify or withdraw consent 7.4.1 Limit collection 8.2.3 Marketing and advertising use
Article 8 Conditions applicable to child's consent in relation to information society services	7.2.2 Identify lawful basis 7.2.3 Determine when and how consent is to be obtained
Article 9 Processing of special categories of personal data	7.2.2 Identify lawful basis 7.2.3 Determine when and how consent is to be obtained 7.2.4 Obtain and record consent
Article 10 Processing of personal data relating to criminal convictions and offences	7.2.2 Identify lawful basis
Article 11 Processing which does not require identification	7.3.2 Determining information for PII principals 7.3.3 Providing information to PII principals 7.4.5 PII de-identification and deletion at the end of processing Control
Article 12 Transparent information, communication and modalities for the exercise of the rights of the data subject	7.3.1 Determining and fulfilling obligations to PII principals 7.3.3 Providing information to PII principals 7.3.9 Handling requests
Article 13 Information to be provided where personal data are collected from the data subject	7.3.2 Determining information for PII principals 7.3.3 Providing information to PII principals 7.3.4 Providing mechanism to modify or withdraw consent 7.3.5 Providing mechanism to object to PII processing 7.3.6 Access, correction and/or erasure 7.3.10 Automated decision making 7.4.7 Retention

GDPR Articles	Applicable ISO 27701 Controls
Article 14 Information to be provided where personal data have not been obtained from the data subject	7.3.2 Determining information for PII principals 7.3.4 Providing mechanism to modify or withdraw consent 7.3.5 Providing mechanism to object to PII processing 7.3.6 Access, correction and/or erasure 7.3.10 Automated decision making 7.4.7 Retention
Article 15 Right of access by the data subject	7.3.2 Determining information for PII principals 7.3.8 Providing copy of PII processed 7.3.9 Handling requests 7.5.1 Indentify basis for PII transfer between jurisidictions 7.5.2 Countries and international organizations to which PII can be transferred 8.3.1 Obligations to PII principles
Article 16 Right to rectification	7.3.6 Access, correction and/or erasure
Article 17 Right to erasure (â€˜right to be forgottenâ€™)	7.2.2 Identify lawful basis 7.3.6 Access, correction and/or erasure 7.3.7 PII controllers' obligations to inform third parties 8.3.1 Obligations to PII principles
Article 18 Right to restriction of processing	77.2.2 Identify lawful basis 7.3.2 Determining information for PII principals 7.3.4 Providing mechanism to modify or withdraw consent
Article 19 Notification obligation regarding rectification or erasure of personal data or restriction of processing	7.3.7 PII controllers' obligations to inform third parties
Article 20 Right to data portability	7.3.8 Providing copy of PII processed
Article 21 Right to object	7.3.2 Determining information for PII principals 7.3.3 Providing information to PII principals 7.3.5 Providing mechanism to object to PII processing

GDPR Articles	Applicable ISO 27701 Controls
Article 22 Automated individual decision-making, including profiling	7.2.2 Identify lawful basis 7.3.10 Automated decision making
Article 23 Restrictions	Jamf monitors restrictions to specific countries data subject processing as applicable.
Article 24 Responsibility of the controller	5.2.1 Understanding the organization and its context 6.2.1.1 Policies for information security 6.15.2.1 Protection of records 7.2.8 Records related to processing PII
Article 25 Data protection by design and by default	5.2.1 Understanding the organization and its context 6.11.2.1 Secure development policy 6.11.2.5 Secure system engineering principles 7.4.2 Limit processing
Article 26 Joint controllers	7.2.7 Joint PII controller
Article 27 Representatives of controllers or processors not established in the Union	6.3.1.1 Information security roles and responsibilities
Article 28 Processor	5.2.1 Understanding the organization and its context 6.10.2.4 Confidentiality or non-disclosure agreements 6.12.1.2 Addressing security within supplier agreements 6.15.1.1 Identification of applicable legislation and contractual requirements 7.2.6 Contracts with PII processors 8.2.1 Customer agreement 8.2.2 Organization's purposes 8.2.4 Infringing instruction 8.2.5 Customer obligations 8.3.1 Obligations to PII principles 8.4.2 Return, transfer or disposal of PII 8.5.4 Notification of PII disclosure requests 8.5.6 Disclosure of subcontractors used to process PII 8.5.7 Engagement of a subcontractor to process PII 8.5.8 Change of subcontractor to process PII

GDPR Articles	Applicable ISO 27701 Controls
Article 29 Processing under the authority of the controller or processor	8.2.2 Organization's purposes
Article 30 Records of processing activities	6.12.1.2 Addressing security within supplier agreements 6.15.1.1 Identification of applicable legislation and contractual requirements 7.2.8 Records related to processing PII 7.5.1 Identify basis for PII transfer between jurisdictions 7.5.2 Countries and international organizations to which PII can be transferred 7.5.3 Records of transfer of PII 7.5.4 Records of PII disclosure to third parties 8.2.6 Records related to processing PII 8.4.2 Return, transfer or disposal of PII 8.5.2 Countries and international organizations to which PII can be transferred 8.5.3 Records of PII disclosure to third parties
Article 31 Cooperation with the supervisory authority	5.2.2 Understanding the needs and expectations of interested parties
Article 32 Security of processing	5.2.4 Information security management system 5.4.1.2 Information security risk assessment 5.4.1.3 Information security risk treatment 6.5.2.1 Classification of information 6.5.3.1 Management of removable media 6.7.1.1 Policy on the use of cryptographic controls 6.9.3.1 Information backup 6.11.1.2 Securing applications services on public networks 6.12.1.2 Addressing security within supplier agreements 6.15.2.1 Independent review of information security 6.15.2.3 Technical compliance review 7.2.1 Identify and document purpose 7.4.5 PII de-identification and deletion at the end of processing Control 8.2.2 Organization's purposes
Article 33 Notification of a personal data breach to the supervisory authority	6.13.1.1 Responsibilities and procedures 6.13.1.5 Respond to information security incidents
Article 34 Communication of a personal data breach to the data subject	6.13.1.1 Responsibilities and procedures 6.13.1.5 Respond to information security incidents

GDPR Articles	Applicable ISO 27701 Controls
Article 35 Data protection impact assessment	5.2.2 Understanding the needs and expectations of interested parties 7.2.5 Privacy impact assessment 8.2.1 Customer agreement
Article 36 Prior consultation	5.2.2 Understanding the needs and expectations of interested parties 7.2.5 Privacy impact assessment
Article 37 Designation of the data protection officer	6.3.1.1 Information security roles and responsibilities
Article 38 Position of the data protection officer	6.3.1.1 Information security roles and responsibilities 6.10.2.4 Confidentiality or non-disclosure agreements
Article 39 Tasks of the data protection officer	6.3.1.1 Information security roles and responsibilities 6.4.2.2 Information security awareness, education and training
Article 40 Codes of conduct	75.2.1 Understanding the organization and its context
Article 41 Monitoring of approved codes of conduct	75.2.1 Understanding the organization and its context
Article 42 Certification	5.2.1 Understanding the organization and its context
Article 43 Certification bodies	Not applicable to Jamf
Article 44 General principle for transfers	7.5.1 Indentify basis for PII transfer between jurisidictions 8.5.1 Basis for PII transfer between jurisdictions

GDPR Articles	Applicable ISO 27701 Controls
Article 45 Transfers on the basis of an adequacy decision	77.5.1 Identify basis for PII transfer between jurisdictions
Article 46 Transfers subject to appropriate safeguards	7.5.1 Identify basis for PII transfer between jurisdictions 8.5.1 Basis for PII transfer between jurisdictions
Article 47 Binding corporate rules	7.5.1 Identify basis for PII transfer between jurisdictions
Article 48 Transfers or disclosures not authorised by Union law	7.5.1 Identify basis for PII transfer between jurisdictions 8.5.1 Basis for PII transfer between jurisdictions 8.5.5 Legally binding PII disclosures
Article 49 Derogations for specific situations	7.5.1 Identify basis for PII transfer between jurisdictions 8.5.1 Basis for PII transfer between jurisdictions
Article 50 International cooperation for the protection of personal data	Not applicable to Jamf