Kofax ControlSuite

Administrator's Guide – Security and Compliance

Version: 1.2.0

Date: 2023-11-23

KOFAX

Table of Contents

Preface

This document describes the security model for Kofax ControlSuite 1.4.0 and provides architecture diagrams and details related to ControlSuite product components. The document also contains essential compliance information about requirements related to the Payment Card Industry Data Security Standard (PCI DSS), the Protected Health Information (PHI) regulated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the General Data Protection Regulation (GDPR) implemented by the European Union (EU), and the California Consumer Privacy Act (CCPA) legislation enacted by the State of California.

Note The information in this document relates to the security model for ControlSuite. For details about ControlSuite features and functionality, please consult your Kofax professional.

Getting help for Kofax products

The Kofax Knowledge Base repository contains articles that are updated on a regular basis to keep you informed about Kofax products. We encourage you to use the Knowledge Base to obtain answers to your product questions.

To access the Kofax Knowledge Base, go to the Kofax website and select Support on the home page.

Note The Kofax Knowledge Base is optimized for use with Google Chrome, Mozilla Firefox, or Microsoft Edge.

The Kofax Knowledge Base provides:

- Powerful search capabilities to help you quickly locate the information you need.

  Type your search terms or phrase into the Search box, and then click the search icon.
- Product information, configuration details and documentation, including release news.

  Scroll through the Kofax Knowledge Base home page to locate a product family. Then click a product family name to view a list of related articles. Please note that some product families require a valid Kofax Portal login to view related articles.
- Access to the Kofax Customer Portal (for eligible customers).

  Click the Customer Support link at the top of the page, and then click Log in to the Customer Portal.
- Access to the Kofax Partner Portal (for eligible partners).

  Click the Partner Support link at the top of the page, and then click Log in to the Partner Portal.
- Access to Kofax support commitments, lifecycle policies, electronic fulfillment details, and self-service tools.

  Scroll to the General Support section, click Support Details, and then select the appropriate tab.

Security and encryption terminology

Access Control List (ACL): Identifies a user (trustee) and specifies the access rights allowed, denied, or audited for that trustee.

Active Directory (AD): Technology created by Microsoft to provide a centralized and standardized system that automates network management of user data, security and distributed resources, and enables interoperation with other directories.

Encrypting File System (EFS): System-level file encryption used to protect data from attacks by unauthorized users who gain physical access to a computer.

Hypertext Transfer Protocol Secure (HTTPS): The use of Secure Socket Layer (SSL) or Transport Layer Security (TLS) as a sublayer under standard HTTP application layering. HTTPS encrypts and decrypts user page requests and the pages that are returned by the Web server.

Internet Printing Protocol Secure (IPPS): Secure/encrypted version of the Internet Printing Protocol, to support the secure transmission of documents for print.

JSON Web Token (JWT): Security token used to authenticate user and service credentials, and permissions to other components within the system.

Public Key Infrastructure (PKI): A security framework that uses two different cryptographic keys, a public key and a private key, to protect communications between clients and servers.

Secure Sockets Layer (SSL): A certificate-based cryptographic protocol that provides encrypted communication and authentication between two entities over the network during transit**.**

SSL Certificate: A security certificate issued by a trusted authority to validate encrypted data.

Transparent Layer Security (TLS): A certificate-based cryptographic protocol that provides encrypted communication and authentication between two entities over the network during transit. TLS is an upgraded successor to SSL.

Security Overview

The ControlSuite security model relies on industry-standard technologies such as Active Directory or LDAP services for authentication and authorization privileges, secure data transmissions using SSL/TLS and encryption such as EFS (Encrypted File System). Information in this document tells how Kofax handles the following aspects of ControlSuite security.

- Authentication and Authorization mechanisms
- Data in transit
- Data at rest

Security Development Lifecycle

Implementation of a Security Development Lifecycle helps software development companies reduce the number of security-related design and coding defects, and the severity of security defects that have not been identified.

The Kofax Security Development Lifecycle is focused on the following areas to ensure security against key vulnerabilities.

- **Risk**: Identify primary and secondary software security risks
- **Product Design**: Address identified risks based on Kofax Security Requirements
- **Verification Techniques**: Use of Kofax tests and activities to verify the corresponding security requirements and vulnerabilities

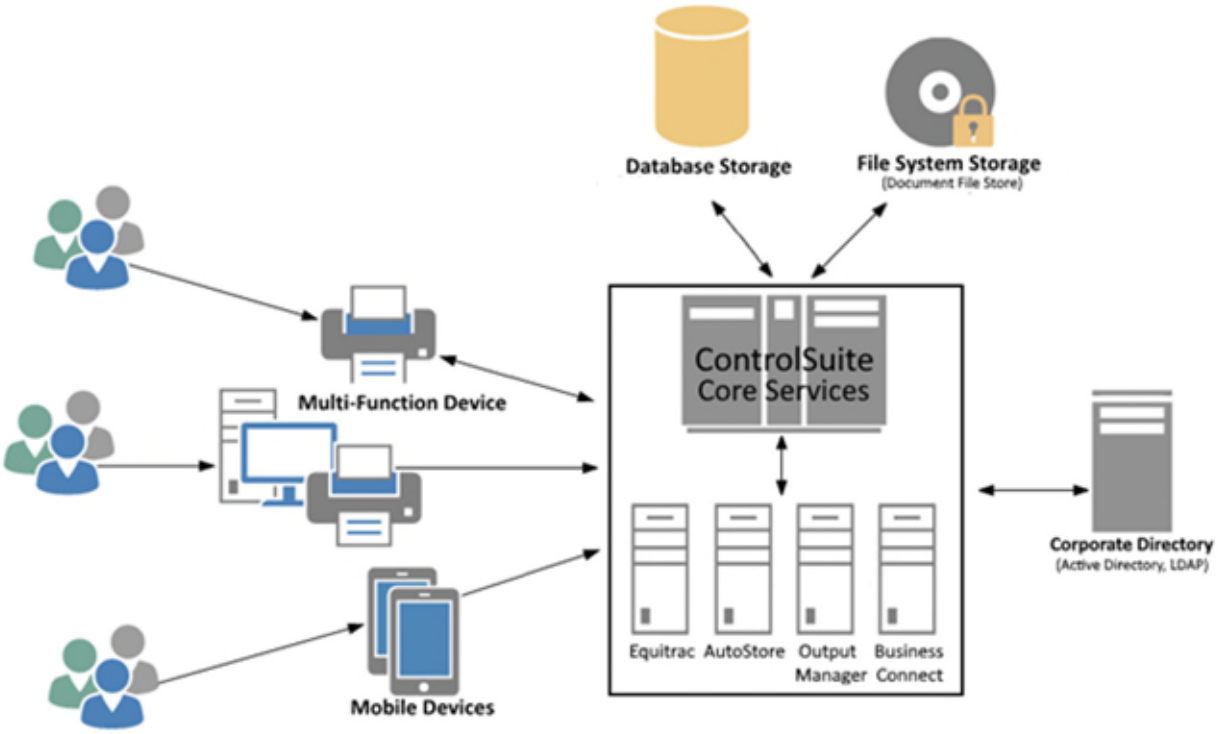
Implementation

Kofax has implemented the following software security best practices.

- Address security considerations across all phases of product development and implementation, including training, planning and design, risk assessment, implementation, verification and testing, and release.
- Regularly review security considerations to ensure continual security improvements.
- Test early and often with a variety of vulnerability tools, network monitoring, and intelligent test cases.

ControlSuite security model

ControlSuite architecture



User login and authentication

Category	Authentication and Authorization
Description	User provides login credentials for ControlSuite application.
Security Details	ControlSuite supports synchronizing users/groups with Active Directory/LDAP. This approach allows ControlSuite to take advantage of the corporate infrastructure for authentication and credential management. ControlSuite also offers application-specific authentication and authorization mechanisms for convenience and added security. These mechanisms include credential management and storage. Stored passwords are encrypted. Once a user has been authenticated, applications send the authenticated user's credentials to the ControlSuite Core Services for authorization. The ControlSuite Core Services first ensure that the application itself is trusted, then generate, sign, and respond with a JSON Web Token (JWT) containing the identity of the user and the roles the user can perform. The application can then call appropriate subcomponents with the JWT authorization. Subcomponents verify the received JWT is signed by a trusted service and contains the necessary permissions to access protected resources. The user's actual credentials are never sent directly to other subcomponents.

Service login and authentication

Category	Authentication and Authorization
Description	ControlSuite service provides credentials to another ControlSuite service.
Security Details	A ControlSuite service will send its credentials to the ControlSuite Core Services, which authenticate the service. The ControlSuite Core Services generate, sign, and respond with a JSON Web Token (JWT) containing the identity of the service and the roles it can perform. The service will then be able to make requests of other ControlSuite services, passing the JWT authorization in place of the credentials. The ControlSuite service receiving the request verifies the received JWT is signed by a trusted service and contains the necessary permissions to access protected resources. The service's actual credentials are never sent directly to other ControlSuite services.

ControlSuite Server transmits to another ControlSuite server

Category	Data in transit
Port	Configurable. Defaults to 8181.
Protocol	HTTPS
Description	ControlSuite server transmits to/from another ControlSuite application or server.
Security Details	All ControlSuite components are configured to use secure encrypted communication (TLS) with custom or administrator supplied certificates. The TLS protocol and cyphers can be configured using Windows settings.

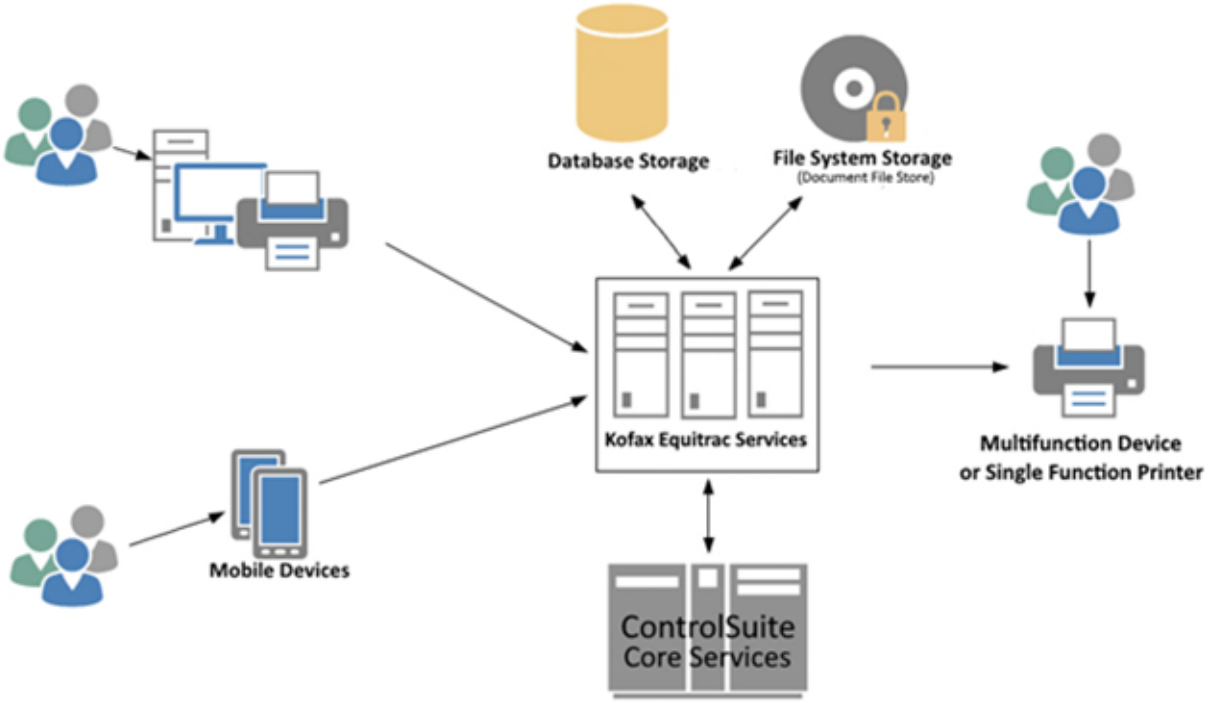
ControlSuite Server transmits to SQL Database server

Category	Data in transit
Port	Varies, depending on protocol
Protocol	TCP/IP or named pipes
Description	ControlSuite servers transmit to/from SQL database.
Security Details	ControlSuite servers connect to an SQL database. Typically, the database server is centrally located, and all deployed security framework nodes communicate with it.

Data storage

Category	Data at rest
Description	Secure storage of component credentials and configuration.
Security Details	ControlSuite service credentials are stored on disk and encrypted. Access control lists (ACLs) limit access to authorized users and services. The configuration for ControlSuite Core Services is stored in the file system and protected by the ACLs.

ControlSuite Print (Equitrac) architecture



Print Subsystem transmits to Equitrac server

Category	Data in transit
Port	Configurable. Defaults to 8181.
Protocol	HTTPS
Description	Windows print spooler transmits print documents to, and receives configuration from, an Equitrac server.
Security Details	All ControlSuite components, including Equitrac, are configured to use secure encrypted communication (TLS) with custom or administrator supplied certificates. The TLS protocol and cyphers can be configured using Windows settings.

Equitrac server transmits to MFD or Single Function Printer

Category	Data in transit
Port	9100, 515 or 631, depending on protocol
Protocol	RAW, LPR, IPP
Description	The Equitrac server transmits print documents to a Multifunction Device (MFD) or Single Function Printer for print.
Security Details	The Equitrac server must connect to the MFD or Single Function Printer to send documents for print. For secure encrypted transmissions, the MFD must support IPPS. Please see the *Print Stream Encryption* document for details on how to configure the print system.

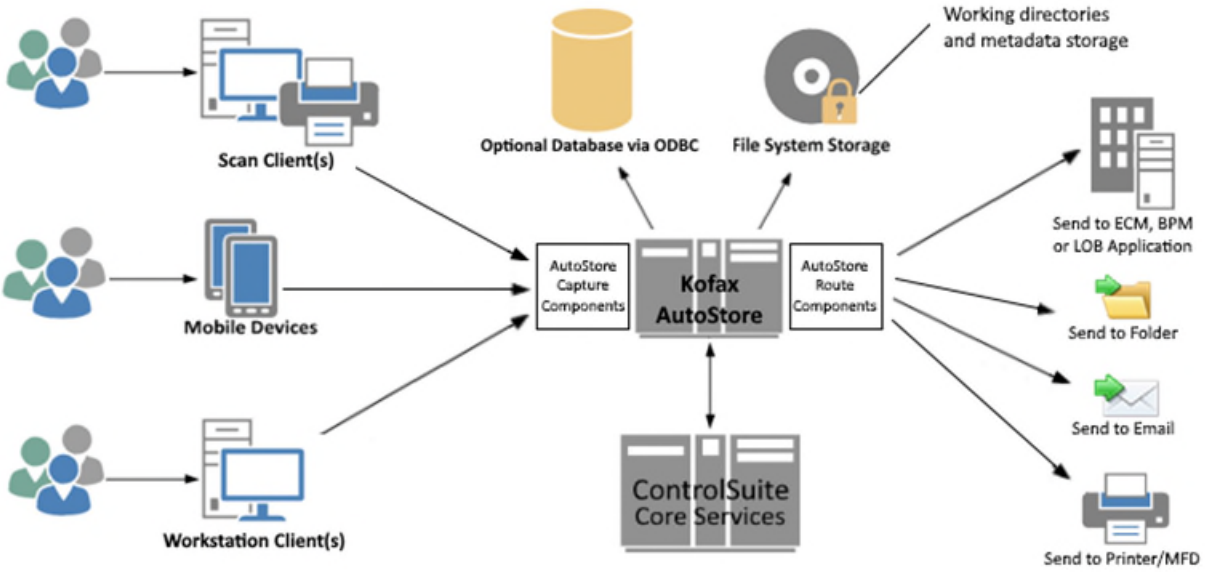
Equitrac Server transmits to Database server

Category	Data in transit
Port	Varies, depending on protocol
Protocol	TCP/IP or named pipes
Description	Equitrac servers transmit to/from database.
Security Details	Equitrac servers connect to a SQL database. Typically, the database server system is co-located with the Equitrac servers that connect to the database.

Data storage

Category	Data at rest
Description	Print documents and metadata stored on disk for secure document release
Security Details	The Equitrac server needs to store printed documents on disk to support page counting and secure document release. Windows Encrypting File System (EFS) should be used to protect the data at rest. Please see the *Print Stream Encryption* document for details on how to configure the print system.

ControlSuite Capture (AutoStore) architecture



Client transmits to AutoStore server

Category	Data in transit
Port	Configurable and depends on the client; see the *AutoStore Communication Port Reference* for details.
Protocol	Depends on the client
Description	The AutoStore client transmits to the AutoStore server.
Security Details	AutoStore capture components can be configured to use secure encrypted communication (TLS) with custom or administrator supplied certificates. The details can be configured using Windows settings.

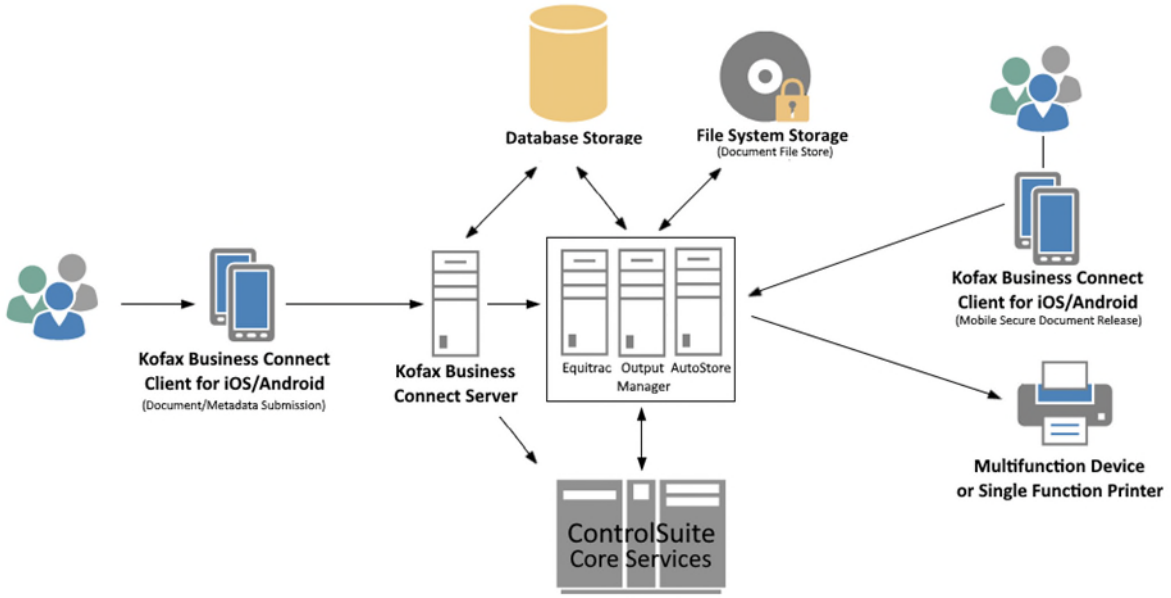
AutoStore Server transmits to Database server (optional)

Category	Data in transit
Port	See *AutoStore Communication Port Reference*
Protocol	TCP/IP or named pipes
Description	The AutoStore server transmits to/from database
Security Details	AutoStore servers can optionally connect to SQL databases. AutoStore uses external databases for data lookup and does not utilize any internal databases.

Data storage

Category	Data at rest
Description	Workflow data stored on disk
Security Details	Documents and metadata submitted to an AutoStore workflow are stored on disk during the workflow execution. Stored passwords are encrypted. Windows Encrypting File System (EFS) should be used to protect the data at rest.

ControlSuite Mobile (Business Connect) architecture



Business Connect mobile application transmits to server

Category	Data in transit
Port	443
Protocol	HTTPS
Description	The Business Connect mobile app transmits to the Business Connect server.
Security Details	Business Connect can be configured to use secure encrypted communication (TLS) with custom or administrator supplied certificates. The details can be configured using Business Connect Configuration Manager, IIS Manager and Windows settings. The only officially supported mode for a production environment is to use an SSL Certificate issued by a trusted Certificate Authority. Self-signed certificates require additional configuration for mobile devices and are not supported. In addition to TLS encryption, user credentials are always encrypted with Public Key Infrastructure (PKI) encryption between the mobile app and the server.

Business Connect server transmits to ControlSuite server

Category	Data in transit
Port	82
Protocol	HTTPS
Description	The Business Connect server transmits to/from other ControlSuite server(s).
Security Details	All ControlSuite components are configured to use secure encrypted communication (TLS) with custom or administrator supplied certificates. The TLS protocol and cyphers can be configured using Windows settings.

Business Connect server transmits to AutoStore WebCapture component

Category	Data in transit
Port	Configurable. Defaults to 3291.
Protocol	HTTPS
Description	The Business Connect server transmits to/from AutoStore WebCapture server.
Security Details	Communication with the AutoStore WebCapture component can be configured to use secure encrypted communication (TLS) with custom or administrator supplied certificates. The TLS protocol and cyphers can be configured using Windows settings.

Business Connect server transmits to Database server

Category	Data in transit
Port	Varies, depending on protocol
Protocol	TCP/IP or named pipes
Description	The Business Connect server transmits to/from database.
Security Details	The Business Connect server can connect to Microsoft SQL Server or Azure SQL database if the SQL Server database is configured instead of the default embedded Microsoft SQL Server Compact Edition database.

ControlSuite Core Services transmit to Database server

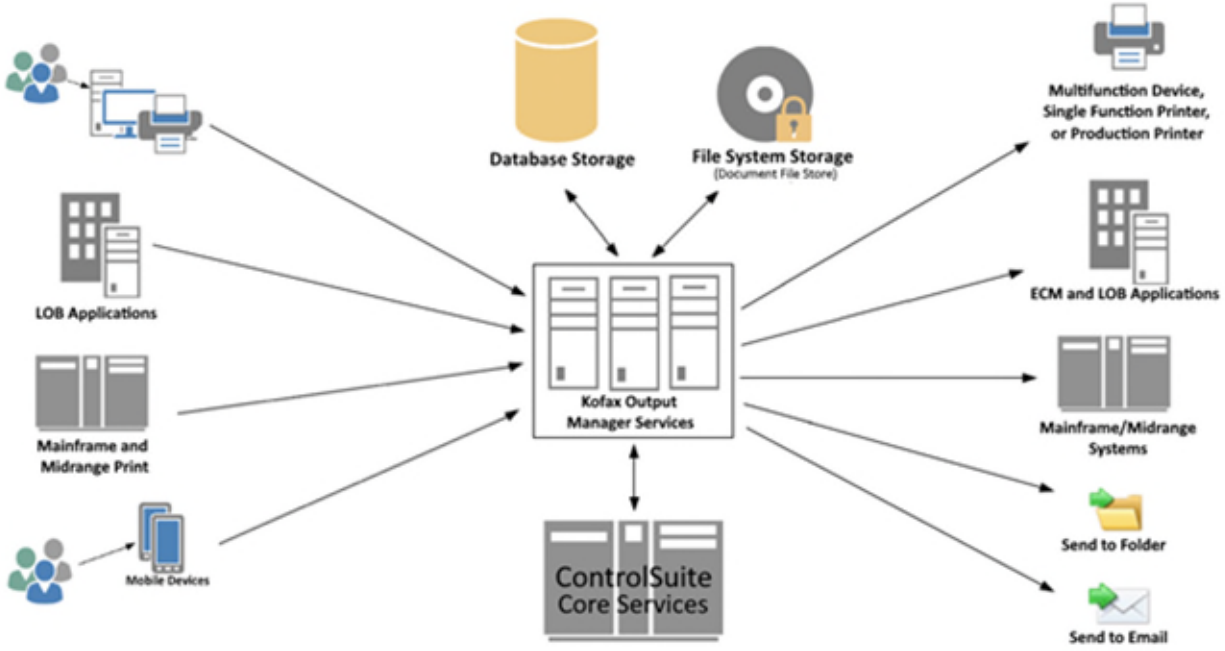
Category	Data in transit
Port	8181
Protocol	HTTPS
Description	ControlSuite Core Services transmit to/from SQL database.
Security Details	Communication from ControlSuite Core Services to SQL server or Azure SQL database and between nodes is configured to use secure encrypted communications with custom self-signed certificates.

Data storage

Category	Data at rest
Description	Primary storage is Microsoft SQL Server Compact Edition database, Azure SQL database or Microsoft SQL Server database. Also, Business Connect stores configuration and some temporary operational data (documents, metadata) in folders that reside within the Windows file system during the workflow execution.

Security Details	By default, the Microsoft SQL Server Compact Edition database is used. The database is always encrypted. The Business Connect server can also be configured to use Microsoft SQL Server database or Azure SQL database. Business Connect servers do not store any credentials or other sensitive data in the database. The Windows Encrypting File System (EFS) should be used to protect the data set stored in the Windows file system at rest.

ControlSuite Output Management (Output Manager) architecture



Applications and clients transmit to Output Manager server

Category	Data in transit
Port	Depends on the client. Common ports include 9100 (Socket), 515 (LPR/LPD), and 631 (IPP)
Protocol	Depends on the client
Description	Output Manager receives data from other applications, clients, and devices through multiple protocols including Native IP Socket, LPR/LPD, and IPP(s). Output Manager receives encrypted information from IPPS clients over secure (TLS) channels.
Security Details	When receiving data from other ControlSuite components, HTTPS is used and secured using custom or administrator supplied certificates. When receiving data from IPP clients, the customer can configure the server to require IPPS (TLS).

Output Manager server to MFD

Category	Data in transit
Port	9100, 515 or 631, depending on protocol
Protocol	RAW, LPR, IPP
Description	The Output Manager server transmits documents to an MFD for print.
Security Details	The Output Manager service needs to connect to the MFD to send print jobs submitted through the system. IPP devices can be configured to support IPPS and Output Manager can be configured to send to these devices over secure (TLS) channels.

Output Manager server transmits to Database server

Category	Data in transit
Port	Varies, depending on protocol
Protocol	TCP/IP or named pipes
Description	The Output Manager server transmits to/from the Database server.
Security Details	The Output Manager server connects to the Microsoft SQL Server database as configured by the Database Administrator.

Data storage

Category	Data at rest
Description	Output Manager stores data in one or more file store folders that reside within the Windows file system.
Security Details	Output Manager provides the ability to encrypt the file store folder using Windows Encrypting File System (EFS).

Payment Card Industry Data Security Standard

The Payment Card Industry Data Security Standard (PCI DSS)[1] governs security requirements for processing payment card data. Its use is mandated by all the major payment card companies. This section provides a high-level overview of PCI DSS and its application to Kofax ControlSuite. This section also summarizes features and functions offered by the Kofax platform, together with the underlying Windows operating system, which facilitates compliance with PCI DSS. Please note that this information details features of software systems and their usage for compliance, rather than specific use cases or compliant implementations of the software; therefore, this information should not be viewed as a statement of compliance with PCI DSS.

PCI DSS is a comprehensive security standard developed as a collaborative effort by the major payment card companies: Visa, MasterCard, American Express, Discover and JCB USA. Implementation of these standards provides an additional level of protection for card issuers by ensuring merchants meet a minimum level of security when they store, process and transmit cardholder data. The Payment Card Industry Security Standards Council (PCI SSC) was formed to maintain and enhance the standard, provide ongoing mitigation of new security risks, and promote the adoption of the PCI DSS.

The following table shows control objectives and associated requirements. The objectives are divided further into more detailed sub-requirements with testing procedures, for more in-depth understanding of the standard.

Control Objective	**Requirement**
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data
	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data
	4. Encrypt transmission of cardholder data across open public networks
Maintain a Vulnerability Management Program	5. Use and regularly update antivirus software or programs
	6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know
	8. Assign a unique ID to each person with system component access
	9. Restrict physical access to cardholder data

[1] http://www.pcisecuritystandards.org

Control Objective	Requirement
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data
	11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Usage and Compliance

While many security practitioners have adopted the core security principles of PCI DSS, mandatory use of the standard is exclusive to cardholder data processing. Payment card companies require PCI DSS compliance for all organizations or merchants, regardless of size or number of transactions, that accept, transmit, or store any cardholder data. The intent of the PCI DSS is not to be a pervasive all-encompassing security standard, and the concept of a *cardholder data environment* is defined where the PCI DSS requirements apply. This allows coexistence with other security processes and procedures within an organization. The cardholder data environment is defined as “the area of computer system network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission.”

Compliance for Merchants

Compliance validation applies to four levels of risk. Merchants base risk levels on transaction volume. The levels range from Level 1 for companies handling over 6,000,000 transactions per year, to Level 4 for companies handling fewer than 20,000 transactions per year. For Level 1, validation requires an annual onsite security audit reviewed by a qualified security assessor (QSA) and quarterly network security scans. The other levels require the completion of an annual self- assessment questionnaire and quarterly network security scans by an approved scanning vendor (ASV).

Exception MasterCard has additional requirements for Level 2 merchants to complete an annual self-assessment questionnaire.

Compliance for Service Providers

A different set of criteria applies to service providers. Service providers process, transmit, and switch transaction and cardholder information, but they are not merchants or card brand members. Hosting-providers and others providing services to merchants would also fall into this category.

Payment brands define service provider compliance.

Example Visa Europe and MasterCard categorize service providers according to transaction volume and/or service provider type, as follows:

Level 1 Criteria

- Visa Europe - Visa System processors or any service provider that stores, processes or transmits more than 300,000 transactions per year.
- MasterCard - All Third Party Processors (TPPs). All Data Storage Entities (DSEs) that store, transmit, or process greater than 300,000 total combined MasterCard and Maestro transactions annually. This includes all compromised DSEs (DSEs where an intrusion has led to suspected unauthorized disclosure, modification, or destruction of cardholder data).

Level 1 Validation Requirements

- Visa Europe - Annual Report on Compliance (ROC) by QSA. Quarterly network scan by Approved Scanning Vendor (ASV). Attestation of Compliance (AOC).
- MasterCard - Annual onsite review by a QSA. Quarterly network scan by an ASV.

Level 2 Criteria

- Visa Europe - Any Service Providers that store, process, or transmit fewer than 300,000 transactions per year.
- MasterCard - All DSE's that store, process, or transmit fewer than 300,000 total combined MasterCard and Maestro transactions annually.

Level 2 Validation Requirements

- Visa Europe - Annual self-assessment questionnaire. Quarterly network scan by an ASV. Attestation of Compliance (AOC).
- MasterCard - Annual self-assessment questionnaire. Quarterly network scan by an ASV.

ControlSuite and PCI DSS

The PCI DSS security standard requirements cover a broad spectrum of security disciplines including security management, policies, procedures, network architecture, software design and other critical protective measures. You can configure ControlSuite using external processing environments to meet PCI DSS compliance.

A ControlSuite solution captures unstructured data in paper and a variety of other formats, classifying and validating that data before transforming the data into actionable information for additional processing. The Kofax solution is not a data repository and does not maintain or store exported data. The information in this section describes PCI DSS compliance in this operating context.

Kofax software uses a Microsoft Windows environment to leverage the underlying functionality of the Windows operating system for base security facilities. For example, Kofax Software uses Active Directory for SSO and is certified to operate with Microsoft EFS subsystems.

- Data in transit
- Data at rest
- Controlling access to data

These concepts are covered in the ControlSuite Security Model section in this document.

ControlSuite and PCI DSS Requirements

Compliance

The PCI DSS requirements are broad and wide ranging. While a number of the requirements involve technology solutions that are addressed directly by the ControlSuite and the underlying operating system, some require measures external to the Kofax platform to ensure compliance. The following table shows how the Kofax platform facilitates, contributes, and requires external measures to meet each requirement.

Facilitated by Kofax platform and Windows operating system
Requires external measures (includes procedural requirements)
Partially facilitated by features in Kofax platform and Windows operating system

Requirement	Sub-requirements									
1. Install and maintain a firewall configuration to protect cardholder data	1.1	1.2	1.3	1.4	1.5					
2. Do not use vendor-supplied defaults for system passwords and other security parameters	2.1	2.2	2.3	2.4	2.5	2.6				
3. Protect stored cardholder data	3.1	3.2	3.3	3.4	3.5	3.6	3.7			
4. Encrypt transmission of cardholder data across open, public networks	4.1	4.2	4.3							
5. Use and regularly update antivirus software or programs	5.1	5.2	5.3	5.4						
6. Develop and maintain secure systems and applications	6.1	6.2	6.3	6.4	6.5	6.6	6.7			
7. Restrict access to cardholder data by business need to know	7.1	7.2	7.3							
8. Assign a unique ID to each person with system component access	8.1	8.2	8.3	8.4	8.5	8.6	8.7	8.8		
9. Restrict physical access to cardholder data	9.1	9.2	9.3	9.4	9.5	9.6	9.7	9.8	9.9	9.10
10. Track and monitor all access to network resources and cardholder data	10.1	10.2	10.3	10.4	10.5	10.6	10.7	10.8		
11. Regularly test security systems and processes	11.1	11.2	11.3	11.4	11.5	11.6				
12. Maintain a policy that addresses information security for all personnel	12.1	12.2	12.3	12.4	12.5	12.6	12.7	12.8	12.9	12.10

Note: The cloud services used by Kofax ControlSuite have been reviewed by an independent Qualified Security Accessor and are determined to be PCI DSS 3.2 compliant.

Objective 1: Build and Maintain Security Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

PCI DSS Requirement 1	Kofax Platform
1.1 Establish firewall and router configuration standards.	Process and procedure, requires measures external to the Kofax platform.
1.2 Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment.	Process and procedure, requires measures external to the Kofax platform.
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	Process and procedure, requires measures external to the Kofax platform.
1.4 Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.	Process and procedure, requires measures external to the Kofax platform.
1.5 Document firewall management security polices and operational procedures and ensure they are in use and known to all affected parties.	Process and procedure, requires measures external to the Kofax platform.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

PCI DSS Requirement 2	Kofax Platform
2.1 Always change vendor-supplied defaults before installing a system on the network—for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.	Process and procedure, requires measures external to the Kofax platform.
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.	Process and procedure, requires measures external to the Kofax platform.
2.3 Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.	The Kofax platform is certified to operate with HTTPS.
2.4 Shared hosting providers must protect each entity's hosted environment and cardholder data.	Process and procedure, requires measures external to the Kofax platform.
2.5 Document management of vendor default security polices and operational procedures and other security parameters, and ensure these are known to all affected parties, and in use.	Process and procedure, requires measures external to the Kofax platform.
2.6 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in the Payment Card Industry (PCI) Data Security Standard document.[2]	Process and procedure, requires measures external to the Kofax platform.

[2] https://www.pcisecuritystandards.org

Objective 2: Protect Cardholder Data

Requirement 3: Protect stored cardholder data

PCI DSS Requirement 3	Kofax Platform
3.1 Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.	The Kofax platform only stores data temporarily during processing and does not need to retain any data post processing. The temporary retention period is configurable by the administrator.
3.2 Do not store sensitive authentication data after authorization (even if encrypted).	In general, ControlSuite does not process card chip data or magnetic strip data other sensitive data such as PINs, PIN blocks, or CVV2, held on paper that may be scanned in as part of processing and can be redacted. Any workflow for scanning reading or processing sensitive information would require a custom solution.
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed).	Some Kofax products and components support redaction (blacking out) of sensitive information held on an image. Please see product-specific documentation for details.
3.4 Render PAN, at minimum, unreadable anywhere it is stored (including on portable digital media, backup media, in logs) by using any of the following approaches: ▪ One-way hashes based on strong cryptography truncation ▪ Index tokens and pads (pads must be securely stored) ▪ Strong cryptography with associated key management processes and procedures	Supported through correct implementation of folder-based encryption using Microsoft EFS and/or database encryption depending on the mix of Kofax Products used.
3.5 Protect cryptographic keys used for encryption of cardholder data against both disclosure and misuse.	Process and procedure, requires measures external to the Kofax platform.
3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data.	Process and procedure, requires measures external to the Kofax platform.
3.7 Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.	Process and procedure, requires measures external to the Kofax platform.

Requirement 4: Encrypt transmission of cardholder data across open public networks

PCI DSS Requirement 4	Kofax Platform
4.1 Use strong cryptography and security protocols such as SSL/TLS to safeguard sensitive cardholder data during transmission over open, public networks. Examples of open, public networks that are in the scope of the PCI DSS include:	Supports the use of HTTPS.

PCI DSS Requirement 4	Kofax Platform
▪ The Internet ▪ Wireless technologies ▪ Global System for Mobile communications (GSM) and General Packet Radio Service (GPRS)	
4.2 Never send unencrypted PANs by end-user messaging technologies (for example, email, instant messaging, or chat).	Standard processing does not require use of messaging technologies.
4.3 Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.	Process and procedure, requires measures external to the Kofax platform.

Objective 3: Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update antivirus software or programs

PCI DSS Requirement 5	Kofax Platform
5.1 Deploy antivirus software on all systems commonly affected by malicious software (particularly personal computers and servers).	Process and procedure, requires measures external to the Kofax platform.
5.2 Ensure that all antivirus mechanisms are current, actively running, and capable of generating audit logs.	Process and procedure, requires measures external to the Kofax platform.
5.3 Ensure that antivirus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.	Process and procedure, requires measures external to the Kofax platform.
5.4 Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.	Process and procedure, requires measures external to the Kofax platform.

Requirement 6: Develop and maintain secure systems and applications

PCI DSS Requirement 6	Kofax Platform
6.1 Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update configuration standards as required by PCI DSS Requirement 2.2 to address new vulnerability issues.	Process and procedure, requires measures external to the Kofax platform.
6.2 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install critical security patches within one month of release.	Process, requires measures external to the Kofax platform.
6.3 Develop software applications in accordance with PCI DSS (for example, secure authentication and logging) and based on industry best practices and incorporate information security throughout software development.	For components developed as part of an implementation process and Procedure, requires measures external to the Kofax platform.

PCI DSS Requirement 6	Kofax Platform
6.4 Follow change control procedures for all changes to system components.	Process and procedures, requires measures external to the Kofax platform.
6.5 Develop all web applications (internal and external and including web administrative access to application) based on secure coding guidelines such as the Open Web Application Security Project Guide. Cover prevention of common coding vulnerabilities in software development	For components developed as part of an implementation process and procedure, requires measures external to the Kofax platform.
6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: ▪ Reviewing public-facing web applications with manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes ▪ Installing a web-application firewall in front of public-facing web applications	Process and procedures, requires measures external to the Kofax platform.
6.7 Document security policies and operational procedures for developing and maintaining secure systems and applications. Ensure these policies and procedures are in use and are known to all affected parties.	Process and procedures, requires measures external to the Kofax platform.

Objective 4: Implement String Access Control Maintenance

Requirement 7: Restrict access to cardholder data by business need to know

PCI DSS Requirement 7	Kofax Platform
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.	Supported by authentication and authorization mechanisms within the Kofax platform and Windows operating system.
7.2 Establish an access control system for system components with multiple users that restricts access based on a user's need to know and is set to **deny all** unless specifically allowed.	Supported by profiles in the Kofax platform and policies within the Windows operating system.
7.3 Document security policies and operational procedures for restricting access to cardholder data. Ensure these policies and procedures are in use and known to all affected parties.	Process and procedures, requires measures external to the Kofax platform.

Requirement 8: Assign a unique ID to each person with system component access

PCI DSS Requirement 8	Kofax Platform
8.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	Supported by Kofax platform.

PCI DSS Requirement 8	Kofax Platform
8.2 In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users: • Password or passphrase • Two-factor authentication (for example, token devices, smart cards, biometrics, or public keys)	Supported by Kofax platform in conjunction with Windows operating system.
8.3 Incorporate two-factor authentication for remote network access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS); terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS) with individual certificates.	Supported by Windows operating system.
8.4 Document and communicate authentication procedures and policies to all users.	Process and procedure, requires measures external to the Kofax platform.
8.5 Do not use group, shared, or generic IDs, passwords or other authentication methods to administer any system components.	Process and procedure, requires measures external to the Kofax platform.
8.6 Where other authentication mechanisms are used, such as physical or logical security tokens, smart cards, or certificates, use of these mechanisms must be assigned as follows: • To an individual account not shared among multiple accounts. • Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.	Process and procedure, requires measures external to the Kofax platform.
8.7 Restrict access to any database containing cardholder data (including access to applications, administrators, and all other users) including the following: • User access to databases through programmatic methods. • Only database administrators can directly access or query databases. • Only applications can use application IDs for databases.	Supported by authentication and authorization mechanisms within the Kofax platform and Windows operating system.
8.8 Document security policies and operational procedures for identification and authentication. Ensure these policies and procedures are in use and known to all affected parties.	Process and procedure, requires measures external to the Kofax platform.

Requirement 9: Restrict physical access to cardholder data

PCI DSS Requirement 9	Kofax Platform
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	Requires measures external to the Kofax platform.
9.2 Develop procedures to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible. For purposes of this requirement, **employee** refers to full-time and part-time employees, temporary employees and personnel, and contractors and consultants who are **resident** on the entity's site. A **visitor** is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the facility for a short duration, usually not more than one day.	Process and procedure, requires measures external to the Kofax platform.
9.3 Make sure all visitors are handled correctly.	Process and procedure, requires measures external to the Kofax platform.
9.4 Use a visitor log to maintain a physical audit trail of visitor activity. Document the visitor's name, the firm represented, and the employee authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.	Process and procedure require measures external to the Kofax platform.
9.5 Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.	Process and procedure, requires measures external to the Kofax platform.
9.6 Physically secure all paper and electronic media that contain cardholder data.	Process and procedure, requires measures external to the Kofax platform.
9.7 Maintain strict control over the internal or external distribution of any kind of media that contains cardholder data.	Process and procedure, requires measures external to the Kofax platform.
9.8 Destroy media containing cardholder data when it is no longer needed for business or legal reasons.	Kofax platform can remove post processed images containing cardholder data. Process and procedure, requires measures external to the Kofax platform to comply generally.
9.9 Maintain strict control over the storage and accessibility of media that contains cardholder data.	Process and procedure, requires measures external to the Kofax platform.
9.10 Document security policies and operational procedures for restricting physical access to cardholder data. Ensure these policies and procedures are in use and known to all affected parties.	Process and procedure, requires measures external to the Kofax platform.

Objective 5: Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

PCI DSS Requirement 10	Kofax Platform
10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	Achieve by defining group policies in Windows operating system and Kofax profiles.
10.1 Implement automated audit trails for all system components.	The Kofax platform can contribute to this requirement but requires measures external to the Kofax platform to fully conform.
10.3 Record audit trail entries for all system components for each event	The Kofax platform can record the required information for its components.
10.4 Synchronize all critical system clocks and times.	Process and procedure, requires measures external to the Kofax platform.
10.5 Secure audit trails so they cannot be altered.	The Kofax platform can contribute to this requirement but requires measures external to the Kofax platform to fully conform.
10.6 Review logs for all system components at least daily. Log reviews must include servers that perform security functions such as intrusion-detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS).	Process and procedure, requires measures external to the Kofax platform.
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	Process and procedure, requires measures external to the Kofax platform.
10.8 Document security policies and operational procedures for monitoring all access to network resources and cardholder data. Ensure these policies and procedures are in use and known to all affected parties.	Process and procedure, requires measures external to the Kofax platform.

Requirement 11: Regularly test security systems and processes

PCI DSS Requirement 11	Kofax Platform
11.1 Test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identify all wireless devices in use.	Process and procedure, requires measures external to the Kofax platform.
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network.	Process and procedure, requires measures external to the Kofax platform.
11.3 Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification.	Process and procedure, requires measures external to the Kofax platform.
11.4 Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic in the cardholder	Process and procedure, requires measures external to the Kofax platform.

PCI DSS Requirement 11	Kofax Platform
data environment and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines up-to-date.	
11.5 Deploy file-integrity monitoring software to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.	Process and procedure, requires measures external to the Kofax platform.
11.6 Document security policies and operational procedures for security monitoring and testing. Ensure these policies and procedures are in use and known to all affected parties.	Process and procedure, requires measures external to the Kofax platform.

Objective 6: Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for all personnel

PCI DSS Requirement 12	Kofax Platform
12.1 Establish, publish, maintain, and disseminate a security policy.	Process and procedure, requires measures external to the Kofax platform.
12.2 Implement a risk assessment process that identifies assets, threats, vulnerabilities, and results and ensure the process is performed at least annually.	Process and procedure, requires measures external to the Kofax platform.
12.3 Develop usage policies for critical employee-facing technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, e-mail usage and Internet usage) to define proper use of these technologies for all employees and contractors.	Process and procedure, requires measures external to the Kofax platform.
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all employees and contractors.	Process and procedure, requires measures external to the Kofax platform.
12.5 Assign information security management responsibilities to an individual or team.	Process and procedure, requires measures external to the Kofax platform.
12.6 Implement a formal security awareness program to make all employees aware of the importance of cardholder data security.	Process and procedure, requires measures external to the Kofax platform.
12.7 Screen potential employees (see definition of **employee** at 9.2 above) prior to hire to minimize the risk of attacks from internal sources. For those employees such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.	Process and procedure, requires measures external to the Kofax platform.

PCI DSS Requirement 12	Kofax Platform
12.8 If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers.	Process and procedure, requires measures external to the Kofax platform.
12.9 Establish a best practice for written acknowledgement of service provider responsibility for the security of cardholder data. **Note:** As of June 30, 2015, this practice is a requirement.	Process and procedure, requires measures external to the Kofax platform.
12.10 Implement an incident response plan. Be prepared to respond immediately to a system breach.	Process and procedure, requires measures external to the Kofax platform.

Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule defines United States national standards protecting electronic personal health information stored by health care providers. HIPAA also requires appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and security of electronic protected health information.

The HIPAA Privacy Rule defines additional privacy standards protecting medical records and other personal health information. The rule requires safeguards to protect patient information sharing without the consent of the patient. The rule applies to providers and their representatives.

Note: HIPAA standards do not specify implementation details. Exact steps to meet HIPAA privacy standards are often left up to companies and/or consulting organizations. As many of the HIPAA requirements are similar to those for the Payment Card Industry Data Security Standard (PCI), Kofax has used PCI requirements as a basis for HIPAA recommendations.

Privacy Rule

The HIPAA Privacy Rule provides standards to protect medical records and other personal health information (PHI) and sets limits on use and disclosure of this information. The Privacy Rule applies to electronic health information (ePHI), as well as oral and written personal health information. These privacy rules also provide individuals with access and correction request rights to their personal health information.

Security Rule

The HIPAA Security Rule establishes standards to protect electronic personal health information (ePHI) that is created, received, used, or maintained by a covered entity. This rule requires sufficient administrative, physical, and technical safeguards to ensure confidentiality, integrity, and security of this information. The Security Rule is more comprehensive than the Privacy Rule, providing detailed requirements specific to ePHI.

ControlSuite and PHI / HIPAA Compliance

The overall IT ramifications of HIPAA are beyond the scope of this document. However, we believe the following topics are key to our customers to meet HIPAA requirements for Kofax ControlSuite.

- Data in transit
- Data at rest
- Audit logging and reporting
- Session timeout

These concepts are covered in the ControlSuite Security Model section of this document.

ControlSuite and HIPAA Security and Privacy

The U.S. Department of Health and Human Services and the Secretary of Health and Human Services maintain national standards and HIPAA rule regulations for electronic health care providers, health insurance providers, and other healthcare industry employers.[3]

The following table shows control objectives and associated recommendations. The objectives are divided further into more detailed sub-recommendations with testing procedures, for more in-depth understanding of the security and privacy standards.

Control Objective	Standard
Administrative Safeguards	1. Security Management
	2. Workforce Security
	3. Information Access Management
	4. Workforce Training
	5. Evaluation and Reporting
	6. Contingency Plan
Physical Safeguards	7. Facility Access Controls
	8. Workstations
	9. Device and Media Controls
Technical Safeguards	10. Access Control
	11. Audit Controls
	12. Authentication
	13. Transmission

Administrative Safeguards

- Security measures with careful consideration of risk and risk management required to protect the data integrity, and privacy while providing secure access to protected health information.
- Actions, policies and procedures required to manage and maintain ePHI security, including workforce management and the reliability of secure access to the data by the appropriate workforce.

Physical Safeguards

- Physical measures, policies and procedures to protect electronic information systems from internal and external risks.
- Security measures to protect related buildings and equipment, from natural and environmental hazards, or unauthorized intrusion.

Technical Safeguards

- Technology, policies, and procedures to control access to ePHI.

[3] https://aspe.hhs.gov/report/health-insurance-portability-and-accountability-act-1996

Kofax Platform and HIPAA Standards

Compliance

HIPAA standards are broad and wide-ranging. While a number of the requirements involve technology solutions that are addressed directly by the Kofax platform and the underlying operating system, some require measures external to the Kofax platform to ensure compliance. The following table shows how the Kofax platform facilitates, contributes, and requires external measures to meet each requirement.

Facilitated by Kofax platform and Windows operating system
Requires external measures (includes procedural requirements)
Partially facilitated by features in Kofax platform and Windows operating system

Requirement	Sub-requirements							
Administrative Safeguards								
1. Security Management Processes	1.1	1.2	1.3	1.4				
2. Workforce Security	2.1	2.2	2.3	2.4				
3. Information Access Management	3.1	3.2	3.3					
4. Workforce Training	4.1	4.2	4.3	4.4	4.5			
5. Evaluation and Reporting	5.1	5.2	5.3					
6. Contingency Plan	6.1	6.2	6.3	6.4	6.5			
Physical Safeguards								
7. Facility Access Control	7.1	7.2	7.3	7.4				
8. Workstations	8.1	8.2						
9. Device and Media Controls	9.1	9.2	9.3	9.4				
Technical Safeguards								
10. Access Control	10.1	10.2	10.3	10.4.a	10.4.b	10.4.c	10.4.d	10.4.e
11. Audit Controls	11.1	11.2	11.3					
12. Authentication	12.1	12.2	12.3					
13. Transmission	13.1	13.2						

Objective 1: Administrative Safeguards (§164.308)

Standard 1: Security Management Processes §164.308(a)(1)

Implement policies and procedures to prevent, detect, contain, and correct security violations.

Note: Implementation Specifications are indicated after each HIPAA standard.

- (R) Required
- (A) Addressable

HIPAA Standard	Kofax Platform
1.1 *Risk Management (R)* —§164.308(a)(1)(ii)(A) & (B); §164.306(a) Assess potential risks to the accessibility, privacy, and reliability of ePHI and implement reasonable security measures.	Process and procedure, requires measures external to the Kofax platform.
1.2 *Sanction Policy (R)* —§164.308(a)(1)(ii)(C) Apply appropriate sanctions against workforce members who fail to comply with security measures.	Process and procedure, requires measures external to the Kofax platform.
1.3 *Information System Activity Review (R)* — §164.308(a)(1)(ii)(D) Implement regular information system activity review.	Process and procedure, requires measures external to the Kofax platform.
1.4 *Assigned Security Responsibility (R)* —§164.308(a)(i)(2) Identify individuals responsible for the design and implementation of security management processes.	Process and procedure, requires measures external to the Kofax platform.

Standard 2: Workforce Security §164.308(a)(3)(i)

Implement policies and procedures to ensure workforce has appropriate access to ePHI.

HIPAA Standard	Kofax Platform
2.1 *Authorization and/or Supervision (A)* —§164.308(a)(3)(i)(A) Define and implement policies and procedures allowing and/or restricting workforce individual's access to ePHI.	Process and procedure, requires measures external to the Kofax platform. **Note**: Kofax Products have user management that allows restricting access to any information stored by Kofax.
2.2 *Workforce Clearance Procedure (A)* —§164.308(a)(3)(i)(B) Implement procedures to determine appropriate access of a workforce member to ePHI.	Process and procedure, requires measures external to the Kofax platform.
2.3 *Termination Procedures (A)* —§164.308(a)(3)(i)(C) Implement procedures regarding termination of access rights to ePHI.	Process and procedure, requires measures external to the Kofax platform.
2.4 *Business Associate Contracts and Other Arrangement (A)* —§164.308(b)(1); §164.314(a) Define and implement policies and procedures to allow a business associate access to ePHI with satisfactory assurance the business associate will safeguard the information.	Process and procedure, requires measures external to the Kofax platform.

Standard 3: Information Access Management §164.308(a)(4)(i)

Implement policies and procedures to authorize access to ePHI.

HIPAA Standard	Kofax Platform
3.1 *Isolating Health Care Clearinghouse Function (R)* —§164.308(a)(4)(ii)(A) Implement policies and procedures to protect ePHI managed by a health care clearinghouse from unauthorized access by the larger organization.	Process and procedure, requires measures external to the Kofax platform.
3.2 *Access Authorization (A)* —§164.308(a)(4)(ii)(B) Implement policies and procedures regarding grant of access rights to ePHI.	Process and procedure, requires measures external to the Kofax platform.
3.3 *Access Establishment and Modification (A)* —§164.308(a)(4)(ii)(C) Implement policies and procedures to document, review, and modify user access to a workstation, transaction, program, or process.	Process and procedure, requires measures external to the Kofax platform.

Standard 4: Workforce Training §164.308(a)(5)

Implement workforce security awareness training including periodic security reminders, protection from malicious software, log-in monitoring, and password management.

HIPAA Standard	Kofax Platform
4.1 *Standard Security awareness training (A)* —§164.308(a)(5)(i) Implement a security awareness and training program for workforce and management.	Process and procedure, requires measures external to the Kofax platform.
4.2 *Security Reminders (A)* —§164.308(a)(5)(i)(A) Periodic security updates.	Process and procedure, requires measures external to the Kofax platform. Kofax Products issue periodic updates, including security updates.
4.3 *Protection from Malicious Software (A)* —§164.308(a)(5)(i)(B) Procedures to guard against, detect, and report malicious software.	Use and regularly update antivirus software or programs Develop and maintain secure systems and applications
4.4 *Log-in Monitoring (A)* —§164.308(a)(5)(i)(C) Procedures to monitor log-in attempts and to report discrepancies.	Process and procedure, requires measures external to the Kofax platform. Supported by Kofax platform in conjunction with Windows operating system.
4.5 *Password Management (A)* —§164.308(a)(5)(i)(D) Procedures to create, change, and safeguard passwords.	Process and procedure, requires measures external to the Kofax platform. Supported by Kofax platform in conjunction with Windows operating system.

Standard 5: Reporting and Evaluation §164.308(a)(6) & §164.308(a)(8)

Implement procedures to evaluate, maintain, and report on established security policies.

HIPAA Standard	Kofax Platform
5.1 *Security Incident Procedures (R)* —§164.308(a)(6)(i) Implement policies and procedures to address security incidents.	Process and procedure, requires measures external to the Kofax platform.
5.2 *Response and Reporting Procedures(R)* —§164.308(a)(6)(ii) Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of known security; and document security incidents and their outcomes.	Kofax platform can contribute to this requirement but requires measures external to the Kofax platform to fully conform.
5.3 *Evaluation (R)* —§164.308(a)(8) In response to environmental or operational changes, perform periodic technical and nontechnical evaluation of ePHI security policies and procedures to determine if they continue to meet requirements.	Process and procedure, requires measures external to the Kofax platform.

Standard 6: Contingency Plan §164.308(a)(1)

Establish policies to protect ePHI during emergencies such as system failure, fire, vandalism, or natural disaster.

HIPAA Standard	Kofax Platform
6.1 *Data Backup Plan (R)* —§164.308(a)(7)(ii)(A) Establish and implement procedures to create and maintain retrievable exact copies of ePHI.	Process and procedure, requires measures external to the Kofax platform.
6.2 *Disaster Recovery Plan (R)* —§164.308(a)(7)(ii)(B) Define procedures to restore any data loss.	Process and procedure, requires measures external to the Kofax platform.
6.3 *Emergency Mode Operation Plan (R)* —§164.308(a)(7)(ii)(C) Define procedures to enable continuation of critical business processes to protect ePHI security while operating in emergency mode.	Process and procedure, requires measures external to the Kofax platform.
6.4 *Testing and Revision Procedure (A)* —§164.308(a)(7)(ii)(D) Implement procedures for periodic tests and revisions of contingency plans.	Process and procedure, requires measures external to the Kofax platform.
6.5 *Applications and Data Criticality Analysis (A)* §164.308(a)(7)(ii)(E)— Implement procedures for periodic contingency plan tests and revisions.	Process and procedure, requires measures external to the Kofax platform.

Objective 2: Physical Safeguards (§164.310)

Limit physical access to electronic information systems and facilities containing ePHI.

Standard 7: Facility Access Controls §164.310(a)(1)

Note: Implementation Specifications are indicated after each HIPAA Standard.

- (R) Required
- (A) Addressable

HIPAA Standard	Kofax Platform
7.1 *Contingency Operations (A)* —§164.310(a)(2)(i) Define a disaster recovery plan to support lost data recovery and emergency mode operations.	Process and procedure, requires measures external to the Kofax platform.
7.2 *Facility Security Plan (A)* —§164.310(a)(2)(ii) Implement facility security policies and procedures to safeguard against unauthorized physical access, tampering, and theft.	Process and procedure, requires measures external to the Kofax platform.
7.3 *Access Control and Validation Procedures (A)* —§164.310(a)(2) (iii) Implement procedures to control and validate facility access, including visitor control and access to software programs for testing and revision.	Process and procedure, requires measures external to the Kofax platform.
7.4 *Maintenance Records (A)* —§164.310(a)(2) (iv) Implement policies and procedures to document facility repairs and modifications to the physical components of a facility related to security such as doors and locks.	Process and procedure, requires measures external to the Kofax platform.

Standard 8: Workstation and Device Security §164.310(b) and (c)

HIPAA Standard	Kofax Platform
8.1 *Workstation Use (R)* —§164.310(b) Implement policies and procedures for proper use of workstations that can access ePHI, including the surrounding area.	Process and procedure, requires measures external to the Kofax platform.
8.2 *Workstation Security (R)* —§164.310(c) Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.	Process and procedure, requires measures external to the Kofax platform. Kofax platform is certified to operate with HTTPS.

Standard 9: Device and Media Controls §164.310(d)(1)

Implement policies and procedures to govern receipt, removal, and movement within the facility of hardware and electronic media containing ePHI.

HIPAA Standard	Kofax Platform
9.1 *Disposal (R)* —§164.310(d)(2)(i) Implement policies and procedures for final disposition of ePHI, and/or the hardware or electronic media on which it is stored.	Process and procedure, requires measures external to the Kofax platform.

HIPAA Standard	Kofax Platform
9.2 *Media Re-use (R)* —§164.310(d)(2)(ii) Implement procedures for removal of ePHI from electronic media.	Process and procedure, requires measures external to the Kofax platform.
9.3 *Accountability (A)* —§164.310(d)(2) (iii) Maintain a record of the movements of hardware and electronic media, including a record of any individual responsible for the movement.	Process and procedure, requires measures external to the Kofax platform.
9.4 *Data Backup and Storage (A)* —§164.310(d)(2) (iv) Create a retrievable, exact ePHI copy, when needed, before movement of equipment.	Process and procedure, requires measures external to the Kofax platform.

Objective 3: Technical Safeguards (§164.312)

Standard 10: Access Control §164.312(a)(1)

Implement technical policies and procedures to maintain electronic information systems containing ePHI.

Note: Implementation Specifications are indicated after each HIPAA Standard.

- (R) Required
- (A) Addressable

HIPAA Standard	Kofax Platform
10.1 *Unique User Identification (R)* —§164.312(a)(2)(i) Assign unique user identity name or number.	Supported by authentication and authorization mechanisms within the Kofax platform and Windows operating system.
10.2 *Emergency Access Procedure (R)* —§164.312(a)(2)(ii) Establish procedures to obtain necessary ePHI during an emergency.	Process and procedure, requires measures external to the Kofax platform. Supported by authentication and authorization mechanisms within the Kofax platform and Windows operating system.
10.3 *Automatic Logoff (A)* —§164.312(a)(2) (iii) Implement electronic procedures to terminate an electronic session after a predetermined period of inactivity.	Process and procedure, requires measures external to the Kofax platform. Supported by authentication and authorization mechanisms within the Kofax platform and Windows operating system.
10.4 *Encryption and Decryption (A)* —§164.312(a)(2) (iv) 10.4.a Implement ePHI encryption and decryption method.	Process and procedure, requires measures external to the Kofax platform.
10.4.b Render personal health information unreadable anywhere it is stored	Supported through correct implementation of folder-based encryption using Microsoft EFS and/or database encryption depending on mix of Kofax Products used.
10.4.c Protect personal health data at rest	Kofax databases are accessed through a configured system account that has ownership of the database or Windows Authentication for the currently logged-in account. The appropriate use of EFS is instrumental in

HIPAA Standard	Kofax Platform
	achieving this goal.
10.4.d Password and server configurations	Kofax databases are accessed through a configured system account that has ownership of the database or Windows Authentication for the currently logged-in account. **Note:** For data in transit, access within a secure intranet configuration may not require encryption.
10.4.e Encrypt transmission of personal health information across open public networks	Kofax supports the use of HTTPS, or site-to-site VPN.

Standard 11: Audit Controls §164.312(b)

Implement hardware, software, and/or procedures to record and examine information system activity containing or using ePHI.

HIPAA Standard	Kofax Platform
11.1 Hardware (R) —§164.312(b)	Process and procedure, requires measures external to the Kofax platform.
11.2 Software (R) —§164.312(b)	Process and procedure, requires measures external to the Kofax platform. Supported by authentication and authorization mechanisms within the Kofax platform and Windows operating system.
11.3 Procedures (R) —§164.312(b)	Process and procedure, requires measures external to the Kofax platform.

Standard 12: Authenticate §164.312(c)(1) and (d)

HIPAA Standard	Kofax Platform
12.1 *Integrity (A)* —§164.312(c)(1) Implement policies and procedures to protect ePHI from improper alteration or destruction.	Process and procedure, requires measures external to the Kofax platform.
12.2 *Mechanism to Authenticate electronic Protected Health Information (A)* —§164.312(c)(1) Implement electronic mechanisms to validate there is no unauthorized ePHI alteration or destruction.	Process and procedure, requires measures external to the Kofax platform.
12.3 *Person or Entity Authentication (R)* —§164.312(d) Implement procedures to verify the identity of the person or entity requesting ePHI access.	Process and procedure, requires measures external to the Kofax platform.

Standard 13: Transmission §164.312(e)(1)

HIPAA Standard	Kofax Platform
13.1 *Integrity Controls (A)* —§164.312(e)(1)(2)(i) Implement security measures to detect improper modification of electronically transmitted ePHI.	Process and procedure, requires measures external to the Kofax platform.
13.2 *Encryption (A)* —§164.312(e)(1)(2)(ii) Implement a mechanism to encrypt electronic ePHI when needed.	Kofax platform operates with TLS and HTTPS.

HIPAA Standard	Kofax Platform
	Supported through correct implementation of folder-based encryption using Microsoft EFS and/or database encryption depending on the mix of Kofax Products used. Kofax databases are accessed through a configured system account that has ownership of the database or Windows Authentication for the currently logged-in account. **Note:** If all access is within a secure intranet configuration, encryption may not be required.

General Data Protection Regulation

The General Data Protection Regulation (GDPR) implemented by the European Union (EU)[4] provides data protection law for all EU Member States and gives control of personal data[5] to the owners. The regulation imposes strict rules for institutions and entities who process and host personal data worldwide. Institutions, businesses, and individuals outside of the EU must also abide by the regulations when they collect or process data for any EU citizen.

Under GDPR, an EU citizen can:

- Review their stored personal data
- Request and receive corrections to their personal data in a timely manner
- Restrict processing of personal data until its accuracy is verified
- Securely move personal data from one IT source to another
- Invoke their right to be forgotten.

Consent

Before processing personal data, institutions and entities must receive consent. The request for consent must clearly explain how the data will be used and how long it will be stored.

- An individual's inactivity or silence is not sufficient compliance for consent.
- Institutions and entities must prove approval to use an individual's personal information.
- Terms of consent must be accurate with the most up-to-date information and individuals must be informed of any changes to the how the data is used.
- Individuals have the right to withdraw consent at any time.
- Institutions and entities must respond to a request to withdraw consent and carry out the request in a reasonable timeframe.

Rectify and amend

Individuals have the right to request corrections and amendments to their personal data. The institution or entity is required to respond to such requests in a timely manner.

Right to be forgotten

Individuals can withdraw consent and request their personal data be deleted. Institutions and entities must remove all traces of the personal data. In addition, data that is no longer used by an institution or entity should be deleted.

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[5] Personal data includes, but is not limited to, names, addresses, identification numbers, images, beliefs, geographic location, IP addresses, ethnicity, race, genetic or biometric data, health, and other data that can identify an individual.

ControlSuite and GDPR Compliance

Compliance

GDPR regulations are broad and wide-ranging. While a number of the requirements involve technology solutions that are addressed directly by the Kofax platform and the underlying operating system, some require measures external to the Kofax platform to ensure compliance.

The overall IT ramifications of GDPR are beyond the scope of this document. However, we believe the following topics are key to our customers to meet GDPR requirements for Kofax Products.

- Data in transit
- Data at rest
- The right to be forgotten
- Permissions

These concepts are covered in the ControlSuite Security Model section of this document.

Requirements

The following table shows the GDPR Control Objective and associated requirements. The requirements are divided further into more detailed regulations in a subsequent section of this document.

Control Objective	Articles
General Provisions	1. Subject-matter and objectives
	2. Material scope
	3. Territorial scope
	4. Definitions
Principles	5. Processing of personal data
	6. Lawfulness of processing
	7. Conditions for consent
	8. Conditions for child's consent
	9. Processing special categories, personal data
	10. Processing personal data relating to criminal convictions and offenses
	11. Processing which does not require identification
Rights of the data subject	12. Transparency and modalities
	13. Information and access to personal data
	14. Information provided when personal data is not obtained from the data subject
	15. Right of access by the data subject
	16. Right to rectification
	17. Right to erasure (right to be forgotten)
	18. Right to restriction of processing
	19. Notification obligation regarding rectification or erasure of personal data or restriction of processing
	20. Right to data portability
	21. Right to object
	22. Automated individual decision-making, including profiling
	23. Restrictions

Control Objective	Standard
Controller and processor	24. Responsibilities of controllers or processors not established in the Union
	25. Data protection by design and by default
	26. Joint controllers
	27. Representatives of controllers or processors not established in the Union
	28. Processor
	29. Processing under the authority of the controller or processor
	30. Records of processing activities
	31. Cooperation with the supervisory authority
	32. Security of processing
	33. Notification of a personal data breach to the supervisory authority
	34. Communication of a personal data breach to the data subject
	35. Data protection impact assessment
	36. Prior consultation
	37. Designation of the data protection officer
	38. Position of the data protection officer
	39. Tasks of the data protection officer
	40. Codes of conduct
	41. Monitoring of approved codes of conduct
	42. Certification
	43. Certification bodies
Transfers of personal data to third countries or international organizations	44. General principle for transfers
	45. Transfers on the basis of an adequacy decision
	46. Transfers subject to appropriate safeguards
	47. Binding corporate rules
	48. Transfers or disclosures not authorized by Union law
	49. Derogations for specific situations
	50. International cooperation for the protection of personal data
Independent supervisory authorities collapse child menu	51. Supervisory authority
	52. Independence
	53. General conditions for the members of the supervisory authority
	54. Rules on the establishment of the supervisory authority
	55. Competence
	56. Competence of the lead supervisory authority
	57. Tasks
	58. Powers
	59. Activity reports

Control Objective	Standard
Cooperation and consistency	60. Cooperation between the lead supervisory authority and the other supervisory authorities concerned
	61. Mutual assistance
	62. Joint operations of supervisory authorities
	63. Consistency mechanism
	64. Opinion of the Board
	65. Dispute resolution by the Board
	66. Urgency procedure
	67. Exchange of information
	68. European Data Protection Board
	69. Independence
	70. Tasks of the Board
	71. Reports
	72. Procedure
	73. Chair
	74. Tasks of the Chair
	75. Secretariat
	76. Confidentiality
Remedies, liability and penalties collapse child menu	77. Right to lodge a complaint with a supervisory authority
	78. Right to an effective judicial remedy against a supervisory authority
	79. Right to an effective judicial remedy against a controller or processor
	80. Representation of data subjects
	81. Suspension of proceedings
	82. Right to compensation and liability
	83. General conditions for imposing administrative fines
	84. Penalties
Provisions relating to specific - processing situations	85. Processing and freedom of expression and information
	86. Processing and public access to official documents
	87. Processing of the national identification number
	88. Processing in the context of employment
	89. Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes
	90. Obligations of secrecy
	91. Existing data protection rules of churches and religious associations
Delegated acts and implementing acts	92. Exercise of the delegation
	93. Committee procedure
Final Provisions	94. Repeal of Directive 95/46/EC
	95. Relationship with Directive 2002/58/EC
	96. Relationship with previously concluded agreements
	97. Commission reports
	98. Review of other Union legal acts on data protection
	99. Entry into force and application

Regulation 1: General provisions

Rules for the protection of personal data during processing and during the free movement of personal data.

Article 1: Subject-matter and objectives

Applicable GDPR Recitals	Kofax Platform
1. Data protection as a fundamental right Protection of personal data is a fundamental right of individuals.	Process and procedure, requires measures external to the Kofax platform. Supported by authentication and authorization mechanisms within the Kofax platform and Windows operating system as well as numerous other Kofax Product features.
2. Respect of the fundamental rights and freedoms	Process and procedure, requires measures external to the Kofax platform.
3. Directive 95/46/EC harmonization Ensure of the free flow of personal data between EU member states when processing personal data.	Process and procedure, requires measures external to the Kofax platform.
4. Data protection in balance with other fundamental rights Protection of data as balanced against other fundamental rights in accordance with the principal of proportionality.	Process and procedure, requires measures external to the Kofax platform.
5. Cooperation between Member States to exchange personal data	Process and procedure, requires measures external to the Kofax platform.
6. Ensuring a high level of data protection despite the increased exchange of data	Process and procedure, requires measures external to the Kofax platform.
7. The framework is based on control and certainty	Process and procedure, requires measures external to the Kofax platform.
8. Adoption into national law	Process and procedure, requires measures external to the Kofax platform.
9. Different standards of protection by the Directive 95/46/EC Consideration of differences in data protection regulations across Member States where differences may constitute and obstacle to the pursuit of economic activities, distort competition, and impede authorities under Union law.	Process and procedure, requires measures external to the Kofax platform.
10. Harmonized level of data protection despite national scope	Process and procedure, requires measures external to the Kofax platform.
11. Harmonization of the powers and sanctions	Process and procedure, requires measures external to the Kofax platform.
12. Authorization of the European Parliament and the Council	Process and procedure, requires measures external to the Kofax platform.

Article 2: Material scope

Processing of personal data by automated or non-automated means

Applicable GDPR Recitals	Kofax Platform
13. Taking account of micro, small and medium-sized enterprises	Process and procedure, requires measures external to the Kofax platform.
14. Not applicable to legal persons	Process and procedure, requires measures external to the Kofax platform.
15. Technology neutrality Protection of personal rights should be technology neutral and not depend on the techniques used.	Process and procedure, requires measures external to the Kofax platform.
16. Not applicable to activities regarding national and common security	Process and procedure, requires measures external to the Kofax platform.
17. Adaptation of Regulation (EC) No 45/2001 Applies to the protection of individuals' personal data by Community institutions and Union entities on the free movement of the data.	Process and procedure, requires measures external to the Kofax platform.
18. Not applicable to personal or household activities The regulation does not apply to the processing of data that is purely personal with no connection to a professional or commercial activity.	Process and procedure, requires measures external to the Kofax platform.
19. Not applicable to criminal prosecution The regulation does not apply to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data.	Process and procedure, requires measures external to the Kofax platform.
20. Respecting the independence of the judiciary	Process and procedure, requires measures external to the Kofax platform.
21. Liability rules of intermediary service providers shall remain unaffected	Process and procedure, requires measures external to the Kofax platform.
27. Not applicable to data of deceased persons	Process and procedure, requires measures external to the Kofax platform.

Article 3: Territorial scope

The processing of personal data within the EU or external to the EU.

Applicable GDPR Recitals	Kofax Platform
22. Processing by an establishment Processing of personal data in the context of the controller or processor within the Union should be carried out in accordance with this regulation.	Process and procedure, requires measures external to the Kofax platform.
23. Applicable to processors not established in the Union if data subjects within the Union are targeted Processing of personal data in the context of the controller or processor not established in the union should be carried out in accordance with this regulation.	Process and procedure, requires measures external to the Kofax platform.

Applicable GDPR Recitals	Kofax Platform
24. Applicable to processors not established in the Union if data subjects within the Union are profiled	Process and procedure, requires measures external to the Kofax platform.
25. Applicable to processors due to international law	Process and procedure, requires measures external to the Kofax platform.

Article 4: Definitions

Applicable GDPR Recitals	Kofax Platform
15. Technology neutrality Protection of personal rights should be technology neutral and not depend on the techniques used.	Process and procedure, requires measures external to the Kofax platform.
24. Applicable to processors not established in the Union if data subjects within the Union are profiled	Process and procedure, requires measures external to the Kofax platform.
26. Not applicable to anonymous data Identifiable information has been replaced with artificial identifiers or pseudonyms.	Process and procedure, requires measures external to the Kofax platform.
28. Introduction of pseudonymization	Process and procedure, requires measures external to the Kofax platform.
29. Pseudonymization at the same controller	Process and procedure, requires measures external to the Kofax platform.
30. Online identifiers for profiling and identifications	Process and procedure, requires measures external to the Kofax platform.
31. Not applicable to public authorities in connection with their official task	Process and procedure, requires measures external to the Kofax platform.
34. Genetic data	Process and procedure, requires measures external to the Kofax platform.
35. Health data	Process and procedure, requires measures external to the Kofax platform.
36. Determination of the main establishment	Process and procedure, requires measures external to the Kofax platform.
37. Enterprise group	Process and procedure, requires measures external to the Kofax platform.

Regulation 2: Principles

Article 5: Principles relating to processing of personal data

Personal data shall be processed lawfully, fairly, with transparency to the individual, limited to the purpose is processed or stored, and ensures appropriate security. Reasonable effort is required to ensure data accuracy and corrections when inaccuracies are known.

Applicable GDPR Recitals	Kofax Platform
39. Principles of data processing	Process and procedure, requires measures external to the Kofax platform. The Kofax products can support these measures as follows: Secure access is supported by authentication and authorization mechanisms within the Kofax platform and Windows operating system. Secure transmission is supported by HTTPS. Secure storage is supported through correct implementation of folder-based encryption using Microsoft EFS and/or database encryption depending on the mix of Kofax Products used.

Article 6: Lawfulness of processing

Applicable GDPR Recitals	Kofax Platform
39. Principles of data processing	Process and procedure, requires measures external to the Kofax platform. The Kofax products can support these measures as follows: Secure access is supported by authentication and authorization mechanisms within the Kofax platform and Windows operating system. Secure transmission is supported by HTTPS. Secure storage is supported through correct implementation of folder-based encryption using Microsoft EFS and/or database encryption depending on the mix of Kofax Products used.
40. Lawfulness of data processing	Process and procedure, requires measures external to the Kofax platform.
41. Legal basis or legislative measures	Process and procedure, requires measures external to the Kofax platform.
42. Burden of proof and requirements for consent	Process and procedure, requires measures external to the Kofax platform.
43. Freely given consent	Process and procedure, requires measures external to the Kofax platform.
44. Performance of a contract	Process and procedure, requires measures external to the Kofax platform.
45. Fulfillment of legal obligations	Process and procedure, requires measures external to the Kofax platform.
46. Vital interests of the data subject	Process and procedure, requires measures external to

Applicable GDPR Recitals	Kofax Platform
	the Kofax platform.
47. Overriding legitimate interest	Process and procedure, requires measures external to the Kofax platform.
48. Overriding legitimate interest within group of undertakings	Process and procedure, requires measures external to the Kofax platform.
49. Network and information security as overriding legitimate interest	Process and procedure, requires measures external to the Kofax platform.
50. Further processing of personal data	Process and procedure, requires measures external to the Kofax platform.
171. Repeal of Directive 95/46/EC and transitional provisions	Process and procedure, requires measures external to the Kofax platform.

Article 7 – Conditions for consent

Individual consent for the collection and processing of personal data.

Applicable GDPR Recitals	Kofax Platform
32. Consent Collected in a non-ambiguous manner.	Process and procedure, requires measures external to the Kofax platform.
33. Consent to certain areas of scientific research	Process and procedure, requires measures external to the Kofax platform.
42. Burden of proof and requirements for consent Held by the institution or entity.	Process and procedure, requires measures external to the Kofax platform.
43. Freely given consent	Process and procedure, requires measures external to the Kofax platform.

Article 8 – Conditions applicable to child's consent in relation to information society services

Applicable GDPR Recitals	Kofax Platform
38. Special protection of children's personal data	Process and procedure, requires measures external to the Kofax platform.

Article 9 – Processing of special categories of personal data

Applicable GDPR Recitals	Kofax Platform
46. Vital interests of the data subject	Process and procedure, requires measures external to the Kofax platform.
51. Protecting sensitive personal data	Process and procedure, requires measures external to the Kofax platform.
52. Exceptions to the prohibition on processing special categories of personal data	Process and procedure, requires measures external to the Kofax platform.
53. Processing of sensitive data in health and social sector	Process and procedure, requires measures external to the Kofax platform.
54. Processing of sensitive data in public health sector	Process and procedure, requires measures external to the Kofax platform.

Applicable GDPR Recitals	Kofax Platform
55. Public interest in processing by official authorities for objectives of recognized religious communities	Process and procedure, requires measures external to the Kofax platform.
56. Processing personal data on people's political opinions by parties	Process and procedure, requires measures external to the Kofax platform.

Article 10 – Processing of personal data relating to criminal convictions and offences

Applicable GDPR Recitals	Kofax Platform
50. Further processing of personal data	Process and procedure, requires measures external to the Kofax platform.

Article 11 – Processing which does not require identification

Processing personal data that no longer requires identification of the individual, the institution or entity is not required to maintain, acquire, or process additional information.

Applicable GDPR Recitals	Kofax Platform
57. Additional data for identification purposes	Process and procedure, requires measures external to the Kofax platform.

Regulation 3: Rights of the data subject

Section 1 – Transparency and modalities

Article 12 – Transparent information, communication and modalities for the exercise of the rights of the data subject

The institution or entity must take appropriate measures to inform the individual in an accessible manner using concise, transparent language.

Applicable GDPR Recitals	Kofax Platform
58. The principle of transparency	Process and procedure, requires measures external to the Kofax platform.
59. Procedures for the exercise of the rights of the data subjects	Process and procedure, requires measures external to the Kofax platform.
60. Information obligation	Process and procedure, requires measures external to the Kofax platform.
73. Restrictions of rights and principles	Process and procedure, requires measures external to the Kofax platform.

Section 2 – Information and access to personal data

Article 13 – Information to be provided where personal data are collected from the data subject

Applicable GDPR Recitals	Kofax Platform
60. Information obligation	Process and procedure, requires measures external to the Kofax platform.
61. Time of information	Process and procedure, requires measures external to

Applicable GDPR Recitals	Kofax Platform
	the Kofax platform.
62. Exceptions to the obligation to provide information	Process and procedure, requires measures external to the Kofax platform.

Article 14 – Information to be provided where personal data have not been obtained from the data subject

Applicable GDPR Recitals	Kofax Platform
60. Information obligation	Process and procedure, requires measures external to the Kofax platform.
61. Time of information	Process and procedure, requires measures external to the Kofax platform.
62. Exceptions to the obligation to provide information	Process and procedure, requires measures external to the Kofax platform.

Article 15 – Right of access by the data subject

Applicable GDPR Recitals	Kofax Platform
63. Right of access	Process and procedure, requires measures external to the Kofax platform.
64. Identity verification	Process and procedure, requires measures external to the Kofax platform.

Section 3 – Rectification and erasure

Article 16 – Right to rectification

Applicable GDPR Recitals	Kofax Platform
65. Right of rectification and erasure	Process and procedure, requires measures external to the Kofax platform. The Kofax platform can help support modification or deletion of field and other data as required.

Article 17 – Right to erasure (“right to be forgotten”)

Applicable GDPR Recitals	Kofax Platform
65. Right of rectification and erasure	Process and procedure, requires measures external to the Kofax platform. The Kofax platform can help support modification or deletion of field and other data as required.
66. Right to be forgotten	Process and procedure, requires measures external to the Kofax platform. The Kofax platform can help support modification or deletion of field and other data as required.

Article 18 – Right to restriction of processing

Applicable GDPR Recitals	Kofax Platform
67. Restriction of processing	Process and procedure, requires measures external to the Kofax platform.

Article 19 – Notification obligation regarding rectification or erasure of personal data or restriction of processing

Applicable GDPR Recitals	Kofax Platform
66. Right to be forgotten	Process and procedure, requires measures external to the Kofax platform. The Kofax platform can help support this.

Article 20 – Right to data portability

Applicable GDPR Recitals	Kofax Platform
68. Right of data portability	Process and procedure, requires measures external to the Kofax platform. The Kofax platform can help support this via support for numerous export formats including in both human and machine-readable formats such as text, Microsoft Excel, email, and others. See specific product documentation for more information on available features applicable to export.

Section 4 – Right to object and automated individual decision-making

Article 21 – Right to object

Applicable GDPR Recitals	Kofax Platform
69. Right to object	Process and procedure, requires measures external to the Kofax platform.
70. Right to object to direct marketing	Process and procedure, requires measures external to the Kofax platform.

Article 22 – Automated individual decision-making, including profiling

Applicable GDPR Recitals	Kofax Platform
71. Profiling	Process and procedure, requires measures external to the Kofax platform.
72. Guidance of the European Data Protection Board regarding profiling	Process and procedure, requires measures external to the Kofax platform.
91. Necessity of a data protection impact assessment	Process and procedure, requires measures external to the Kofax platform.

Section 5 – Restrictions

Article 23 – Restrictions

An institution or entity may restrict the scope of the obligations and rights through legislative measures in cases of national security, defense, and public security, investigation of criminal offences, matters of public health, or judicial proceedings.

Applicable GDPR Recitals	Kofax Platform
73. Restriction of rights and principles	Process and procedure, requires measures external to the Kofax platform.

Regulation 4: Controller and processor

Section 1 – General obligations

Article 24 – Responsibility of the controller

Applicable GDPR Recitals	Kofax Platform
74. Responsibility and liability of the controller	Process and procedure, requires measures external to the Kofax platform.
75. Risks to the rights and freedoms of natural persons	Process and procedure, requires measures external to the Kofax platform.
76. Risk assessment	Process and procedure, requires measures external to the Kofax platform.
77. Risk assessment guidelines	Process and procedure, requires measures external to the Kofax platform.

Article 25 – Data protection by design and by default

Applicable GDPR Recitals	Kofax Platform
78. Appropriate technical and organizational measures	Supported by Kofax platform in conjunction with Windows operating system and measures external to the Kofax platform.

Article 26 – Joint controllers

Applicable GDPR Recitals	Kofax Platform
79. Allocation of the responsibilities	Process and procedure, requires measures external to the Kofax platform.

Article 27 – Representatives of controllers or processors not established in the Union

Applicable GDPR Recitals	Kofax Platform
80. Designation of a representative	Process and procedure, requires measures external to the Kofax platform.

Article 28 – Processor

Institution or entity's use of processors must implement appropriate technical and organizational measures are followed to ensure the protection of the rights of the individual.

Applicable GDPR Recitals	Kofax Platform
81. The use of processors	Process and procedure, requires measures external to the Kofax platform.

Article 29 – Processing under the authority of the controller or processor

Process and procedure, requires measures external to the Kofax platform.

Article 30 – Records of processing activities

Institutions and entities shall maintain record of processing activities under its responsibility.

Applicable GDPR Recitals	Kofax Platform
13. Taking account of micro, small and medium-sized enterprises	Process and procedure, requires measures external to the Kofax platform.
82. Record of processing activities	Process and procedure, requires measures external to the Kofax platform. The Kofax platform can help support this.

Article 31 – Cooperation with the supervisory authority

Institutions and entities shall cooperate on request with supervisory authority in the performance of its tasks.

Applicable GDPR Recitals	Kofax Platform
82. Record of processing activities	Process and procedure, requires measures external to the Kofax platform. The Kofax platform can help support this.

Section 2 – Security of personal data

Article 32 – Security of processing

Institutions and entities shall implement appropriate measures to ensure an appropriate level of security.

Applicable GDPR Recitals	Kofax Platform
75. Risks to the rights and freedoms of natural persons	Process and procedure, requires measures external to the Kofax platform.
76. Risk assessment	Process and procedure, requires measures external to the Kofax platform.
77. Risk assessment guidelines	Process and procedure, requires measures external to the Kofax platform.
78. Appropriate technical and organizational measures	Process and procedure, requires measures external to the Kofax platform.
79. Allocation of the responsibilities	Process and procedure, requires measures external to the Kofax platform.

Applicable GDPR Recitals	Kofax Platform
83. Security of processing	Process and procedure, requires measures external to the Kofax platform. The Kofax products can support these measures as follows: Secure access is supported by authentication and authorization mechanisms within the Kofax platform and Windows operating system. Secure transmission is supported by HTTPS. Secure storage is supported through correct implementation of folder-based encryption using Microsoft EFS and/or database encryption depending on the mix of Kofax Products used.

Article 33 – Notification of a personal data breach to the supervisory authority

Institutions and entities shall notify individuals of any personal data breach without undue delay.

Applicable GDPR Recitals	Kofax Platform
85. Notification obligation of breaches to the supervisory authority	Process and procedure, requires measures external to the Kofax platform.
87. Promptness of reporting / notification	Process and procedure, requires measures external to the Kofax platform.
88. Format and procedures of the notification	Process and procedure, requires measures external to the Kofax platform.

Article 34 – Communication of a personal data breach to the data subject

Applicable GDPR Recitals	Kofax Platform
86. Notification obligation of breaches to the supervisory authority	Process and procedure, requires measures external to the Kofax platform.
87. Notification of data subjects in case of data breaches	Process and procedure, requires measures external to the Kofax platform.
88. Promptness of reporting / notification	Process and procedure, requires measures external to the Kofax platform.

Section 3 – Data protection impact assessment and prior consultation

Article 35 – Data protection impact assessment

Applicable GDPR Recitals	Kofax Platform
75. Risks to the rights and freedoms of natural persons	Process and procedure, requires measures external to the Kofax platform.
84. Risk evaluation and impact assessment	Process and procedure, requires measures external to the Kofax platform.
89. Elimination of the general reporting requirement	Process and procedure, requires measures external to the Kofax platform.
90. Data protection impact assessment	Process and procedure, requires measures external to the Kofax platform.
91. Necessity of a data protection impact assessment	Process and procedure, requires measures external to

Applicable GDPR Recitals	Kofax Platform
	the Kofax platform.
92. Broader data protection impact assessment	Process and procedure, requires measures external to the Kofax platform.
93. Data protection impact assessment at authorities	Process and procedure, requires measures external to the Kofax platform.

Article 36 – Prior consultation

Applicable GDPR Recitals	Kofax Platform
94. Consultation of the supervisory authority	Process and procedure, requires measures external to the Kofax platform.
95. Support by the processor	Process and procedure, requires measures external to the Kofax platform.
96. Consultation of the supervisory authority in the course of a legislative process	Process and procedure, requires measures external to the Kofax platform.

Section 4 – Data protection officer

Article 37 – Designation of the data protection officer

Applicable GDPR Recitals	Kofax Platform
97. Data protection officer	Process and procedure, requires measures external to the Kofax platform.

Article 38 – Position of the data protection officer

Applicable GDPR Recitals	Kofax Platform
97. Data protection officer	Process and procedure, requires measures external to the Kofax platform.

Article 39 – Tasks of the data protection officer

Applicable GDPR Recitals	Kofax Platform
97. Data protection officer	Process and procedure, requires measures external to the Kofax platform.

Section 5 – Codes of conduct and certification

Article 40 – Codes of conduct

Applicable GDPR Recitals	Kofax Platform
98. Preparation of codes of conduct by organizations and associations	Process and procedure, requires measures external to the Kofax platform.
99. Consultation of stakeholders and data subjects in the development of codes of conduct	Process and procedure, requires measures external to the Kofax platform.

Article 41 – Monitoring of approved codes of conduct

No applicable regulations associated with this Article.

Article 42 – Certification

Member States and supervisory authorities shall encourage establishment of data protection certification for the purpose of demonstrating compliance.

Applicable GDPR Recitals	Kofax Platform
100. Certification	Process and procedure, requires measures external to the Kofax platform.

Article 43 – Certification bodies

Note: Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).

Regulation 5: Transfers of personal data to third countries or international organizations

Article 44 – General principle for transfers

Institutions and entities should get an individual's permission before transferring data.

Applicable GDPR Recitals	Kofax Platform
101. General principles for international data transfers	Process and procedure, requires measures external to the Kofax platform.
102. International agreements for an appropriate level of data protection	Process and procedure, requires measures external to the Kofax platform.

Article 45 – Transfers on the basis of an adequacy decision

Applicable GDPR Recitals	Kofax Platform
103. Appropriate level of data protection based on an adequacy decision	Process and procedure, requires measures external to the Kofax platform.
104. Criteria for an adequacy decision	Process and procedure, requires measures external to the Kofax platform.
105. Consideration of international agreements for an adequacy decision	Process and procedure, requires measures external to the Kofax platform.
106. Monitoring and periodic review of the level of data protection	Process and procedure, requires measures external to the Kofax platform.
107. Amendment, revocation and suspension of adequacy decisions	Process and procedure, requires measures external to the Kofax platform.

Article 46 – Transfers subject to appropriate safeguards

Applicable GDPR Recitals	Kofax Platform
108. Appropriate safeguards	Process and procedure, requires measures external to the Kofax platform.

Applicable GDPR Recitals	Kofax Platform
109. Standard data protection clauses	Process and procedure, requires measures external to the Kofax platform.

Article 47 – Binding corporate rules

Applicable GDPR Recitals	Kofax Platform
110. Binding corporate rules	Process and procedure, requires measures external to the Kofax platform.

Article 48 – Transfers or disclosures not authorized by Union law

Applicable GDPR Recitals	Kofax Platform
115. Rules in third countries contrary to the Regulation	Process and procedure, requires measures external to the Kofax platform.

Article 49 – Derogations for specific situations

Applicable GDPR Recitals	Kofax Platform
111. Exceptions for certain cases of international transfers	Process and procedure, requires measures external to the Kofax platform.
112. Data transfers due to important reasons of public interest	Process and procedure, requires measures external to the Kofax platform.
113. Transfers qualified as not repetitive and that only concern a limited number of data subjects	Process and procedure, requires measures external to the Kofax platform.
114. Safeguarding of enforceability of rights and obligations in the absence of an adequacy decision	Process and procedure, requires measures external to the Kofax platform.
115. Rules in third countries contrary to the Regulation	Process and procedure, requires measures external to the Kofax platform.

Article 50 – International cooperation for the protection of personal data

Applicable GDPR Recitals	Kofax Platform
116. Cooperation among supervisory authorities	Process and procedure, requires measures external to the Kofax platform.

Regulation 6: Independent supervisory authorities

Section 1 – Independent status

The agency that monitors GDPR within a country.

Article 51 – Supervisory authority

Applicable GDPR Recitals	Kofax Platform
117. Establishment of supervisory authorities	Process and procedure, requires measures external to the Kofax platform.
118. Monitoring of the supervisory authorities	Process and procedure, requires measures external to the Kofax platform.

Applicable GDPR Recitals	Kofax Platform
119. Organization of several supervisory authorities of a Member State	Process and procedure, requires measures external to the Kofax platform.
120. Features of supervisory authorities	Process and procedure, requires measures external to the Kofax platform.

Article 52 – Independence

Applicable GDPR Recitals	Kofax Platform
117. Establishment of supervisory authorities	Process and procedure, requires measures external to the Kofax platform.
118. Monitoring of the supervisory authorities	Process and procedure, requires measures external to the Kofax platform.
120. Features of supervisory authorities	Process and procedure, requires measures external to the Kofax platform.
121. Independence of the supervisory authorities	Process and procedure, requires measures external to the Kofax platform.

Article 53 – General conditions for the members of the supervisory authority

Applicable GDPR Recitals	Kofax Platform
121. Independence of the supervisory authorities	Process and procedure, requires measures external to the Kofax platform.

Article 54 – Rules on the establishment of the supervisory authority

Applicable GDPR Recitals	Kofax Platform
117. Establishment of supervisory authorities	Process and procedure, requires measures external to the Kofax platform.
121. Independence of the supervisory authorities	Process and procedure, requires measures external to the Kofax platform.

Section 2 – Competence, tasks and powers

Regulatory authorities within a country should have sufficient expertise in technical areas such as encryption, data storage, and data transfer.

Article 55 – Competence

Applicable GDPR Recitals	Kofax Platform
122. Independence of the supervisory authorities	Process and procedure, requires measures external to the Kofax platform.

Article 56 – Competence of the lead supervisory authority

Applicable GDPR Recitals	Kofax Platform
124. Lead authority regarding processing in several Member States	Process and procedure, requires measures external to the Kofax platform.

Applicable GDPR Recitals	Kofax Platform
127. Information of the supervisory authority regarding local processing	Process and procedure, requires measures external to the Kofax platform.
128. Responsibility regarding processing in the public interest	Process and procedure, requires measures external to the Kofax platform.

Article 57 – Tasks

Applicable GDPR Recitals	Kofax Platform
122. Responsibility of the supervisory authorities	Process and procedure, requires measures external to the Kofax platform.
123. Cooperation of the supervisory authorities with each other and with the Commission	Process and procedure, requires measures external to the Kofax platform.
132. Awareness-raising activities and specific measures	Process and procedure, requires measures external to the Kofax platform.
133. Mutual assistance and provisional measures	Process and procedure, requires measures external to the Kofax platform.
137. Provisional measures	Process and procedure, requires measures external to the Kofax platform.

Article 58 – Powers

Applicable GDPR Recitals	Kofax Platform
122. Responsibility of the supervisory authorities	Process and procedure, requires measures external to the Kofax platform.
129. Tasks and powers of the supervisory authorities	Process and procedure, requires measures external to the Kofax platform.
131. Attempt of an amicable settlement	Process and procedure, requires measures external to the Kofax platform.

Article 59 – Activity reports

No applicable regulations associated with this Article.

Regulation 7: Cooperation and consistency

Section 1 – Cooperation

Article 60 – Cooperation between the lead supervisory authority and the other supervisory authorities concerned

Applicable GDPR Recitals	Kofax Platform
124. Lead authority regarding processing in several Member States	Process and procedure, requires measures external to the Kofax platform.
125. Competences of the lead authority	Process and procedure, requires measures external to the Kofax platform.
130. Consideration of the authority with which the complaint has been lodged	Process and procedure, requires measures external to the Kofax platform.

Article 61 – Mutual assistance

Applicable GDPR Recitals	Kofax Platform
123. Cooperation of the supervisory authorities with each other and with the Commission	Process and procedure, requires measures external to the Kofax platform.
132. Awareness-raising activities and specific measures	Process and procedure, requires measures external to the Kofax platform.
133. Mutual assistance and provisional measures	Process and procedure, requires measures external to the Kofax platform.

Article 62 – Joint operations of supervisory authorities

Applicable GDPR Recitals	Kofax Platform
126. Joint decisions	Process and procedure, requires measures external to the Kofax platform.
134. Participation in joint operations	Process and procedure, requires measures external to the Kofax platform.

Section 2 – Consistency

Article 63 – Consistency mechanism

Applicable GDPR Recitals	Kofax Platform
135. Consistency mechanism	Process and procedure, requires measures external to the Kofax platform.

Article 64 – Opinion of the Board

Applicable GDPR Recitals	Kofax Platform
136. Binding decisions and opinions of the Board	Process and procedure, requires measures external to the Kofax platform.

Article 65 – Dispute resolution by the Board

Applicable GDPR Recitals	Kofax Platform
136. Binding decisions and opinions of the Board	Process and procedure, requires measures external to the Kofax platform.

Article 66 – Urgency procedure

Applicable GDPR Recitals	Kofax Platform
137. Provisional measures	Process and procedure, requires measures external to the Kofax platform.
138. Urgency procedure	Process and procedure, requires measures external to the Kofax platform.

Article 67 – Exchange of information

Refers to the standardized format defined in Article 63 and implemented in Article 93(2).

Section 3 – European data protection board

Article 68 – European Data Protection Board

Applicable GDPR Recitals	Kofax Platform
139. European Data Protection Board	Process and procedure, requires measures external to the Kofax platform.

Article 69 – Independence

Applicable GDPR Recitals	Kofax Platform
139. European Data Protection Board	Process and procedure, requires measures external to the Kofax platform.

Article 70 – Tasks of the Board

Applicable GDPR Recitals	Kofax Platform
136. Binding decisions and opinions of the Board	Process and procedure, requires measures external to the Kofax platform.
139. European Data Protection Board	Process and procedure, requires measures external to the Kofax platform.

Article 71 – Reports

Defines activities of the European Data Protection Board that are external to the Kofax platform.

Article 72 – Procedure

Defines activities of the European Data Protection Board that are external to the Kofax platform.

Article 73 – Chair

Defines activities of the European Data Protection Board that are external to the Kofax platform.

Article 74 – Tasks of the Chair

Defines activities of the European Data Protection Board that are external to the Kofax platform.

Article 75 – Secretariat

Applicable GDPR Recitals	Kofax Platform
140. Secretariat and staff of the Board	Process and procedure, requires measures external to the Kofax platform.

Article 76 – Confidentiality

Defines activities of the European Data Protection Board that are external to the Kofax platform.

Regulation 8: Remedies, liability and penalties

Article 77 – Right to lodge a complaint with a supervisory authority

Applicable GDPR Recitals	Kofax Platform
141. Right to lodge a complaint	Process and procedure, requires measures external to the Kofax platform.

Article 78 – Right to an effective judicial remedy against a supervisory authority

Applicable GDPR Recitals	Kofax Platform
141. Right to lodge a complaint	Process and procedure, requires measures external to the Kofax platform.
143. Judicial remedies	Process and procedure, requires measures external to the Kofax platform.

Article 79 – Right to an effective judicial remedy against a controller or processor

Applicable GDPR Recitals	Kofax Platform
141. Right to lodge a complaint	Process and procedure, requires measures external to the Kofax platform.
145. Choice of venue	Process and procedure, requires measures external to the Kofax platform.

Article 80 – Representation of data subjects

Applicable GDPR Recitals	Kofax Platform
142. The right of data subjects to mandate a not-for-profit body, organization, or association	Process and procedure, requires measures external to the Kofax platform.

Article 81 – Suspension of proceedings

Applicable GDPR Recitals	Kofax Platform
144. Related proceedings	Process and procedure, requires measures external to the Kofax platform.

Article 82 – Right to compensation and liability

Applicable GDPR Recitals	Kofax Platform
145. Choice of venue	Process and procedure, requires measures external to the Kofax platform.
146. Indemnity	Process and procedure, requires measures external to the Kofax platform.
147. Jurisdiction	Process and procedure, requires measures external to the Kofax platform.

Article 83 – General conditions for imposing administrative fines

Applicable GDPR Recitals	Kofax Platform
148. Penalties	Process and procedure, requires measures external to the Kofax platform.
149. Penalties for infringements of national rules	Process and procedure, requires measures external to the Kofax platform.
150. Administrative fines	Process and procedure, requires measures external to the Kofax platform.
151. Administrative fines in Denmark and Estonia	Process and procedure, requires measures external to the Kofax platform.

Applicable GDPR Recitals	Kofax Platform
152. Power of sanction of the Member States	Process and procedure, requires measures external to the Kofax platform.

Article 84 – Penalties

Applicable GDPR Recitals	Kofax Platform
149. Penalties for infringements of national rules	Process and procedure, requires measures external to the Kofax platform.
150. Administrative fines	Process and procedure, requires measures external to the Kofax platform.
151. Administrative fines in Denmark and Estonia	Process and procedure, requires measures external to the Kofax platform.
152. Power of sanction of the Member States	Process and procedure, requires measures external to the Kofax platform.

Regulation 9: Provisions relating to specific processing situations

Article 85 – Processing and freedom of expression and information

Applicable GDPR Recitals	Kofax Platform
153. Processing of personal data solely for journalistic purposes or for the purposes of academic, artistic or literary expression	Process and procedure, requires measures external to the Kofax platform.

Article 86 – Processing and public access to official documents

Applicable GDPR Recitals	Kofax Platform
154. Principle of public access to official documents	Process and procedure, requires measures external to the Kofax platform.

Article 87 – Processing of the national identification number

Defines activities of Member States that are external to the Kofax platform.

Article 88 – Processing in the context of employment

Applicable GDPR Recitals	Kofax Platform
155. Processing in the employment context	Process and procedure, requires measures external to the Kofax platform.

Article 89 – Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

Applicable GDPR Recitals	Kofax Platform
156. Processing for archiving, scientific or historical research or statistical purposes	Process and procedure, requires measures external to the Kofax platform.
157. Information from registries and scientific research	Process and procedure, requires measures external to the Kofax platform.
158. Processing for archiving purposes	Process and procedure, requires measures external to

Applicable GDPR Recitals	Kofax Platform
	the Kofax platform.
159. Processing for scientific research purposes	Process and procedure, requires measures external to the Kofax platform.
160. Processing for historical research purposes	Process and procedure, requires measures external to the Kofax platform.
161. Consenting to the participation in clinical trials	Process and procedure, requires measures external to the Kofax platform.
162. Processing for statistical purposes	Process and procedure, requires measures external to the Kofax platform.
163. Production of European and national statistics	Process and procedure, requires measures external to the Kofax platform.

Article 90 – Obligations of secrecy

Applicable GDPR Recitals	Kofax Platform
164. Professional or other equivalent secrecy obligations	Process and procedure, requires measures external to the Kofax platform.

Article 91 – Existing data protection rules of churches and religious associations

Applicable GDPR Recitals	Kofax Platform
165. No prejudice of the status of churches and religious associations	Process and procedure, requires measures external to the Kofax platform.

Regulation 10: Delegated acts and implementing acts

Article 92 – Exercise of the delegation

Applicable GDPR Recitals	Kofax Platform
166. Delegated acts of the Commission	Process and procedure, requires measures external to the Kofax platform.
167. Implementing powers of the Commission	Process and procedure, requires measures external to the Kofax platform.
168. Implementing acts on standard contractual clauses	Process and procedure, requires measures external to the Kofax platform.
169. Immediately applicable implementing acts	Process and procedure, requires measures external to the Kofax platform.
170. Principle of subsidiarity and principle of proportionality	Process and procedure, requires measures external to the Kofax platform.

Article 93 – Committee procedure

Defines activities of the Commission that are external to the Kofax platform.

Regulation 11: Final provisions

Article 94 – Repeal of Directive 95/46/EC

GDPR cancels this earlier EU regulation.

Applicable GDPR Recitals	Kofax Platform
171. Repeal of Directive 95/46/EC and transitional provisions	Process and procedure, requires measures external to the Kofax platform.

Article 95 – Relationship with Directive 2002/58/EC

GDPR integrates with this earlier EU regulation.

Applicable GDPR Recitals	Kofax Platform
173. Relationship to Directive 2002/58/EC	Process and procedure, requires measures external to the Kofax platform.

Article 96 – Relationship with previously concluded Agreements

GDPR cancels previous international agreements.

Process and procedure, requires measures external to the Kofax platform.

Article 97 – Commission reports

The Commission is required to report on GDPR every four years.

Process and procedure, requires measures external to the Kofax platform.

Article 98 – Review of other Union legal acts on data protection

Process and procedure, requires measures external to the Kofax platform.

Article 99 – Entry into force and application

GDPR effective date – May 25, 2018.

California Consumer Privacy Act

The California Consumer Privacy Act (CCPA) is a state law intended to enhance privacy rights and consumer protection for residents of California in the United States. CCPA applies to any person or entity that conducts business in California and satisfies at least one of the following requirements:

- Has annual gross revenues in excess of $25 million
- Buys, receives, or sells the personal information of 50,000 or more consumers or households
- Earns more than half of its annual revenue from selling consumers' personal information

Privacy rights

Under CCPA, consumers have certain rights related to their personal information collected by and on behalf of a business subject to the law. Personal information may include data elements such as geolocation, IP address, biometric information, professional or employment-related information, education information, browsing and search history, and other noted types of data.

Consumers have certain rights under CCPA to expect that businesses implement reasonable security, as outlined in the following sections.

Right to know personal information

Under CCPA, California residents may request a business to disclose the following information about the business' collection and use of their personal information over the past twelve (12) months, provided that such requests are made no more than twice within a twelve (12) month period:

- The categories of personal information collected
- The categories of sources for the personal information collected
- The business or commercial purpose for collecting, and, if applicable, selling, personal information
- The specific pieces of personal information collected
- If the personal information has been disclosed, the categories of personal information disclosed and the categories of third parties receiving the personal information
- If the personal information has been sold, the categories of personal information sold and the categories of third parties to whom the personal information was sold.

Right of deletion

California residents may request a business to delete the personal information that the business collected and has been retained by the business or its service providers. This right is limited, and the business may deny a deletion request if it is necessary for the business or a service provider to maintain the personal information in order to:

- Complete the transaction for which the personal information was collected, provide a good or service requested by the individual, or reasonably anticipated within the context of a business' ongoing business relationship with the individual, or otherwise perform a contract between the business and the individual.

- Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.
- Debug to identify and repair errors that impair existing intended functionality
- Comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code.
- Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest, where the businesses' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the individual has provided informed consent.
- Enable solely internal uses that are reasonably aligned with the expectations of the individual based on the individual's relationship with the business.
- Comply with a legal obligation.
- Otherwise use the individual's personal information, internally, in a lawful manner that is compatible with the purpose for which the individual provided the information.

Right of no sale of personal information

A California resident has the right to opt-out of the sale of their Personal Information by a business subject to the CCPA. In addition, a business subject to the CCPA must have affirmative authorization in order to sell the Personal Information of a California resident who it knows is under the age of 16.

Right of Non-Discrimination

A business subject to the CCPA may not discriminate against a California resident for exercising any of their CCPA privacy rights.

ControlSuite and CCPA Compliance

Compliance

CCPA regulations are broad and wide-ranging. While some CCPA requirements involve technology solutions addressed directly by the Kofax platform and the underlying operating system, most require measures external to the Kofax platform to ensure compliance.

The overall IT ramifications of CCPA are beyond the scope of this document. However, we believe the following topics are key to our customers to meet CCPA requirements for Kofax Products.

- Data in transit
- Data at rest
- Data privacy rights

These concepts are covered in the ControlSuite Security Model section of this document.

Requirements

Under CCPA, organizations are expected to implement a certain level of controls that enforce reasonable security relative to collection or maintenance of personal information. The following table shows the minimum level of Center for Internet Security (CIS) Controls that must be implemented under CCPA.

CIS Control Title	Action	CIS Control References
General Provisions	Know the hardware and software connected to your network.	CSC 1, CSC 2
Configure Securely	Implement key security settings.	CSC 3, CSC 11
Control Users	Limit user and administrator privileges.	CSC 5, CSC 14
Update Continuously	Continuously assess vulnerabilities and patch holes to stay current.	CSC 4
Protect Key Assets	Secure critical assets and attack vectors.	CSC 7, CSC 10, CSC 13
Implement Defenses	Defend against malware and boundary intrusions.	CSC 8, CSC 12
Block Access	Block vulnerable access points.	CSC 9, CSC 15, CSC 18
Train Staff	Provide security training to employees, contractors and any vendors with access.	CSC 17
Monitor Activity	Monitor accounts and network audit logs.	CSC 6, CSC 16
Test and Plan Response	Conduct tests of your defenses and be prepared to respond promptly and effectively to security incidents.	CSC 19, CSC 20

Recommended measures

In addition to CIS Controls, the California Attorney General has recommended implementation of three measures listed in the following table.

Title	Action
Multi-Factor Authentication	Multi-factor authentication should be available to consumer-facing online accounts in addition to employee systems. Multi-factor authentication pairs “something you know,” such as a password or PIN, with “something you are or have,” such as your cell phone or fingerprint.
Encryption of Data on Portable Devices	Use encryption on laptops and other portable devices.
Fraud Alerts	Inform consumers about placing a fraud alert on their credit files when there is a breach.

ControlSuite and CCPA requirements

This section summarizes how CCPA requirements are addressed by Kofax ControlSuite.

CCPA Requirement	Kofax Platform
General Provisions, CSC 1, CSC 2 Know the hardware and software connected to your network.	Process and procedure, requires measures external to the Kofax platform. See Security Development Lifecycle for more information about implementation and methodology applied during development of Kofax products.
Configure Securely, CSC 3, CSC 11 Implement key security settings.	Kofax platform is certified to operate with HTTPS. Supported through correct implementation of folder-based encryption using Microsoft EFS and/or database encryption depending on mix of Kofax Products used. Kofax databases are accessed through a configured system account that has ownership of the database or Windows Authentication for the currently logged-in account. **Note**: If all access is within a secure intranet configuration, encryption may not be required.
Control Users, CSC 5, CSC 14 Limit user and administrator privileges.	Supported by authentication and authorization mechanisms within the Kofax platform and Windows operating system as well as numerous other Kofax Product features. **Note**: Kofax Products provide user management that allows restricting access to any information stored by Kofax.
Update Continuously, CSC 4 Continuously assess vulnerabilities and patch holes to stay current.	Kofax supports several features and add-on products that can be used to monitor for vulnerabilities.
Protect Key Assets, CSC 7, CSC 10, CSC 13 Secure critical assets and attack vectors.	Process and procedure, requires measures external to the Kofax platform.
Implement Defenses, CSC 8, CSC 12 Defend against malware and boundary intrusions.	Process and procedure, requires measures external to the Kofax platform.
Block Access, CSC 9, CSC 15, CSC 18 Block vulnerable access points.	Process and procedure, requires measures external to the Kofax platform. Supported by Kofax platform in conjunction with Windows operating system.
Train Staff, CSC 17 Provide security training to employees, contractors and any vendors with access.	Process and procedure, requires measures external to the Kofax platform.
Monitor Activity, CSC 6, CSC 16 Monitor accounts and network audit logs.	Process and procedure, requires measures external to the Kofax platform. The Kofax platform can help support this.

CCPA Requirement	Kofax Platform
Test and Plan Response, CSC 19, CSC 20 Conduct tests of your defenses and be prepared to respond promptly and effectively to security incidents.	Process and procedure, requires measures external to the Kofax platform. The Kofax platform can help support this.
Multi-Factor Authentication Multi-factor authentication should be available to consumer-facing online accounts in addition to employee systems. Multi-factor authentication pairs “something you know,” such as a password or PIN, with “something you are or have,” such as your cell phone or fingerprint.	Supported by authentication and authorization mechanisms from the Windows operating system. Multi-factor authorization is supported using mobile devices, RFID card swipes, etc. in conjunction with passwords and PINs. See Overview for additional information. **Note**: Kofax products provide user management that allows restricting access to any information stored by Kofax as linked or synchronized to users in the Windows operating system.
Encryption of Data on Portable Devices Use encryption on laptops and other portable devices.	Kofax platform is certified to operate with HTTPS. Supported through correct implementation of folder-based encryption using Microsoft EFS and/or database encryption depending on the mix of Kofax Products used. Kofax databases are accessed through a configured system account that has ownership of the database or Windows Authentication for the currently logged-in account. **Note**: If all access is within a secure intranet configuration, encryption may not be required.
Fraud Alerts Inform consumers about placing a fraud alert on their credit files when there is a breach.	Process and procedure, requires measures external to the Kofax platform.