File Transfer and the GDPR

General Data Protection Regulation Article 32 (2):

"In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to ***personal data transmitted, stored or otherwise processed.***"

Progress® | ipswitch®

Preparing for GDPR

The General Data Protection Regulation (GDPR) has been accepted by the European Parliament and Council and becomes law on May 25, 2018. The GDPR sets a high standard for data protection and applies to any organisation that processes, or controls the processing of, the personal data of EU residents. Failure to comply with the GDPR can result in penalties of € 20 million or 4% of worldwide annual turnover, whichever amount is greater.

The GDPR defines two types of organisations whose activities are regulated; Controllers and Processors. A processor is any organisation that collects, processes, stores or transmits personal data of EU citizens. A controller is an organisation that directs the processors activities. This extends the responsibility of the original data collector (the controller in this case) to the actual processing of data by an outsourcer or business partner (the processor). Under GDPR, both collectors and processors are responsible for data protection and both are subject to fines for non-compliance. In Controller/Processor relationships, it behooves both parties to coordinate compliance efforts with regards to data transfers. Whichever side of the equation they fall on, organisations will need to review (and likely improve) their data protection controls, processes and technology. In this undertaking, efforts should be guided by Article 32 of the GDPR which requires that the level of security implemented is appropriate to the risk.

ARTICLE 32(1):

CONTROLLERS AND PROCESSORS MUST 'ENSURE A LEVEL OF SECURITY APPROPRIATE TO THE RISK'.

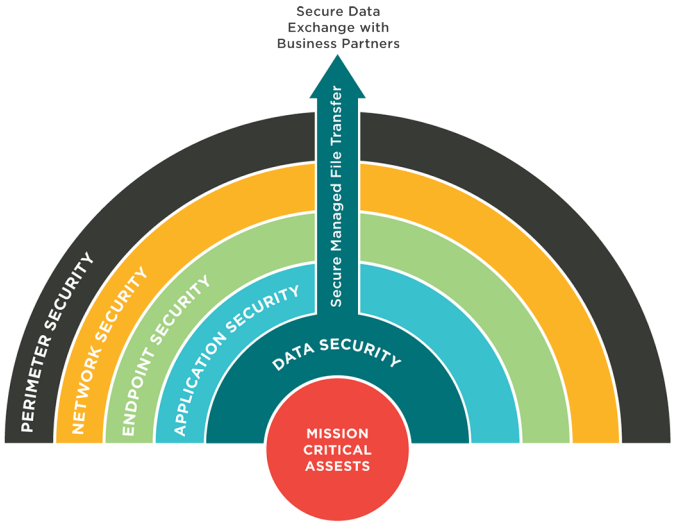
ARTICLE 32(2):

'ACCOUNT SHALL BE TAKEN IN PARTICULAR OF THE RISKS PRESENTED ... FROM ACCIDENTAL, LOSS, ALTERATION, UNAUTHORISED DISCLOSURE OF, OR ACCESS TO PERSONAL DATA TRANSMITTED, STORED OR OTHERWISE PROCESSED.'

File Transfers are High Risk

Chances are your organisation has already invested substantially in a security infrastructure. GDPR requires the consideration of value provided by further expenditures in traditional areas versus training for personnel, new processes and technology investment requirements that have been overlooked.

The external transfer of personal data is now a core operational business process of IT organisations across a wide variety of industries. From a security



ARTICLE 4(2):

"PROCESSING" MEANS ANY OPERATION ... SUCH AS COLLECTION, RECORDING, ORGANISATION, STRUCTURING, STORAGE... TRANSMISSION, DISSEMINATION OR OTHERWISE MAKING AVAILABLE

perspective, data in transit is data at risk as it presents a unique opportunity for interception in transmission, unauthorised access when stored for download on a transfer server, delivery to an unintended recipient or mishandling when processed at its destination.

Clearly, external file transfers of personal data require considerable attention in preparation for GDPR. Under pressure to allocate limited time and resources, organisations need to focus their GDPR investments on the processing activities that pose the greatest risk to their sensitive personal data.

Data transfer is explicitly identified as a processing activity under GDPR, and for good reason. Data transfer activities can expose personal data to high risk. For example:

- Personal data stored in files uploaded to FTP are unencrypted and rarely deleted
- FTP anonymous mode, out-of-date security patches and other vulnerabilities provide easy access to cybercriminals
- Desktop users may circumvent IT and send personal data over unsecured means such as email or cloud-based file share services
- Lack of centralised control over permissions exposes user credentials which hackers can exploit to gain control over protected data.
- Lack of centralised and tamper evident audit logs creates a risk of unauthorised or failed transfers going unnoticed.

GDPR Data Protection Principles

The GDPR lists Data Protection Principles that organisations must comply with. Many of these principles apply to personal data transfer activities.

Fair, lawful and transparent processing	Rec 39, Art 5(1)(a)	Additional care when designing and implementing processing activities
Data Security	Rec 29, 71, 156 Art 5(1)(f), 24(1), 25(1,2), 28, 29, 32	Ensuring personal data are secure against internal and external treats, accidental loss, destruction and damage
Accuracy	Rec 39, Art 5(1)(d)	Taking all reasonable steps to ensure that personal data is accurate
Accountability	Rec 85, Art 5(2)	Demonstrating compliance with the Data Protection Principles
Purpose limitation	Rec 50, Art 5(1)(b)	Personal data collected for one purpose should not be used for a new incompatible purpose
Data minimisation	Rec 39, Art 5(1)(c)	Only processing the personal data it needs to achieve its purposes
Retention periods	Rec 39, Art 5(1)(e)	Personal data should not be retained longer than needed for purpose

Secure FTP Servers are Not Compliant

Attempting to upgrade an existing FTP environment to be GDPR compliant is a flawed strategy. You would have to assure that all external transfer processes use secure protocols (SFTP, FTPS and HTTPS) and encryption (SSH, TLS and SSL). You would also have to add AES-256 encryption to all upload processes to protect data at rest. However, these improvements are not enough. Secure FTP inherits many of the risks and vulnerabilities as the FTP servers they replace.

If your organisation has experienced "FTP sprawl", you may have a hodgepodge of FTP servers with different software, on different platforms, with different software revisions, OS revisions and security patches. This creates vulnerabilities that cybercriminals can exploit to access personal data.

	Secure FTP								Scripts			
	Protects Data in Transit	Protects Data at Rest	File Integrity Checking	Non-repudiation	Content Scanning	Gateway Proxy Server	Ad Hoc File Transfer	Fine Grained Access Control	Tamper Evident Audit Logs	Task-based File Transfer	Centralized Control	Real-time Alerts	Analytics
Data Security	✓		✓									✓	
Purpose of Limitation Principle													
Data Minimization													
Accuracy													
Data Retention Periods													
Accountability	✓		✓										
Fair, Lawful and Transparent Processing	✓		✓										

FTP data transfers are typically reliant on scripts. Scripts can be written in different languages such as PERL, BASH, VB and PowerShell and are often undocumented. Without standardisation and centralised control, scripted workflows, installed across multiple FTP servers, can result in unauthorised processing of personal data.

And lastly, GDPR requires IT and security teams to provide proof of compliance. Collecting and reporting on audit logs from multiple FTP servers is time consuming and raises red flags with auditors who have a

AVOID FTP SERVER SPRAWL

- X FILES ARE UNENCRYPTED
- X LOGS ARE NOT CENTRALISED
- X SCRIPTS MAY BE UNDOCUMENTED
- X AUDITORS WILL BE SUSPICIOUS

preference for a single source of log data in a consistent format and stored in a tamper-evident database.

Addressing these limitations will require considerable time and expense to get data transfer environments up to GDPR standards. The question is "Why would you want to?" Another consideration is that under GDPR, auditors are going to have less tolerance for compensating controls.

How MOVEit Can Help

GDPR Data Protection Principle: Fair and Lawful Processing, Data Security and Accuracy

MOVEit provides security features to meet specific requirements called out in Articles 5, 24, 25, 28, 32 and 39 including:

- √ Encrypting personal data in transit and at rest.
- √ Non-repudiation to validate that personal data is transferred only between authorised senders and receivers.
- √ Integration with Data Loss Prevention and Anti-virus solutions.
- √ Browser and Microsoft Outlook integration to ensure desktop clients are using an IT authorised secure data transfer solution.
- √ Perimeter security to keep unencrypted personal data out of the DMZ.
- √ Centralised, fine grained access control to safeguard user credentials, permissions and personal data.

MOVEit protects personal data in transit using secure data transfer protocols like SFTP, FTPS and HTTPS, as well as the SSH, TLS and SSL encryption protocols. MOVEit protects data at rest using AES-256 encryption.

MOVEit's non-repudiation capability validates that personal data is only transferred between authorised senders and receivers. It is a safeguard against man-in-the-middle attacks, where data in transit is hijacked or tampered with. Automatic file integrity checking validates that a file has not been altered in any way - an additional safeguard for the GDPR Accuracy Principle.

It provides additional protection by integrating with content scanning solutions like Data Loss Prevention (DLP) and Anti-Virus software. It logs all content scanning activities and alerts when data loss or malware is detected.

The Progress Gateway is a proxy server that sits in the DMZ ensuring that no personal data is stored in the DMZ. It terminates all inbound connections in the DMZ and makes sure that all communications to the trusted network go through a secure tunnel.

Ad Hoc functionality delivers easy to learn and use data transfer for desktop clients. Users can send large files securely through a web browser or Microsoft Outlook. This reduces the chances of users exposing sensitive data by circumventing IT with unsecured cloud-based file share solutions.

MOVEit has its own built-in secure database, which is used to safeguard user credentials and permissions. Because of its unique combination of encrypted storage and secure permissions, it does not rely on the security of the underlying OS, where hackers can exploit known vulnerabilities

GDPR Data Protection Principle: Accountability

The principle of Accountability require organisations to demonstrate compliance with the GDPR Data Protection Principles. Organisations need to collect and secure audit trails of all data transfer activities involving personal data. MOVEit tracks all file transfer activities including authentications and modifications to workflows in a tamper-evident database.

MOVEit automatically collects and reports on data transfer logs – in one centralised consolidated location. MOVEit audit logs are tamper evident and can be trusted for accuracy.

GDPR Data Protection Principles: Purpose Limitation, Data Minimisation and Data Retention Periods

The principles of the Purpose of Limitation, Data Minimisation and Data Retention Periods limits the processing of personal data for a specific purpose and to only provide the data needed for that purpose, after which the data must be deleted.

MOVEit replaces scripts with a forms-based solution that provides a standardised, more secure, and documented data transfer tasks. MOVEit centralises control over all data transfer activities. Its built-in scheduler enables organisations to schedule common repetitive data transfer tasks. Organisations can include post transfer tasks, such as the scheduled deletion of personal data files. Comprehensive analytics provide the required insights to transfer activities to assure on-going compliance with GDPR's data protection principles.

MOVEit's Adherence to the GDPR's Data Protection Principles

The lowest risk, cost effective option is a managed data transfer solution like Ipswitch MOVEit. MOVEit is a centralised and consolidated data transfer solution. It integrates secure data transfer with centralised workflows, access control, and audit logging. It features turnkey high availability and failover. The result, fewer moving parts which translates into lower risk to personal data, and less time and money spent managing and supporting data transfer processing activities.

	MOVEit Transfer								MOVEit Automation				
	Protects Data in Transit	Protects Data at Rest	File Integrity Checking	Non-repudiation	Content Scanning	Gateway Proxy Server	Ad Hoc File Transfer	Fine Grained Access Control	Tamper Evident Audit Logs	Task-based File Transfer	Centralised Control	Real-time Alerts	Analytics
Data Security	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Purpose of Limitation Principle									✓	✓	✓		✓
Data Minimisation									✓	✓	✓		✓
Accuracy			✓	✓	✓				✓				
Data Retention Periods									✓	✓	✓		✓
Accountability	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Fair, Lawful and Transparent Processing	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓

About Progress

Progress (NASDAQ: PRGS) offers the leading platform for developing and deploying strategic business applications. We enable customers and partners to deliver modern, high-impact digital experiences with a fraction of the effort, time and cost. Progress offers powerful tools for easily building adaptive user experiences across any type of device or touchpoint, the flexibility of a cloud-native app dev platform to deliver modern apps, leading data connectivity technology, web content management, business rules, secure file transfer, network monitoring, plus award-winning machine learning that enables cognitive capabilities to be a part of any application. Over 1,700 independent software vendors, 100,000 enterprise customers, and two million developers rely on Progress to power their applications. Learn about

Progress at www.progress.com or +1-800-477-6473.

Progress® MOVEit®

Download your FREE TRIAL of MOVEit