ipswitch

Secure. Control. Perform.

AN IPSWITCH WHITEPAPER

# 7 Steps to Compliance with GDPR

## How the General Data Protection Regulation Applies to External File Transfers

ipswitch

# Introduction

Stolen personal data drives a thriving black market for cybercriminals on a global basis. Typically defined as any data which can be used to identify an individual - this makes every organization that collects information such as passwords, credit card numbers, health information or addresses a prime target for cybercriminals. Not surprisingly, since 2013 data breaches have accounted for nearly 6 billion stolen data records globally.

In response to this increasing threat, the European Commission put forward the General Data Protection Regulation (GDPR) which has since been accepted by the European Parliament and Council and becomes law on May 25, 2018. The GDPR replaces the 20-year-old Data Protection Directive, strengthens many of the Directive's original clauses and sets an higher standard for the protection of EU residents' personal data.

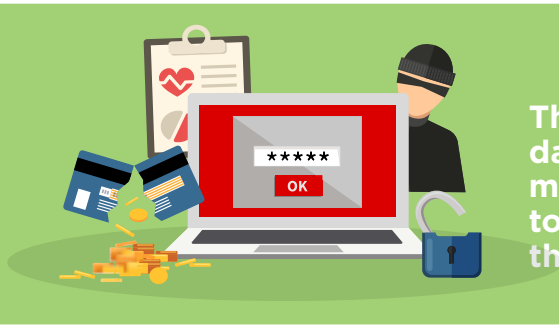
The external transfer of personal data is now a core operational business process of IT organizations across a wide variety of industries. From a security perspective, data in transit is data at risk as it presents a unique opportunity for interception in transmission or when stored and processed at its destination.

In preparation for GDPR, IT organizations involved in external transfers of personal data should review the seven security controls listed in this whitepaper. They are widely considered best practices in assuring security before, during and after the external transfer of protected data.

# The Threat

Personal data is typically defined as any data which by itself, or when combined with other data that the possessor can likely access, can be used to identify an individual. To a cybercriminal, the collection, processing and transfer of personal data makes organizations across a large number of industries lucrative targets for phishing, denial of service, ransomware and advanced persistent threat attacks.

Since 2013, publicly recorded data breaches have accounted for over 5.8 billion lost records globally. The data lost includes passwords, health records, billing addresses and credit information.




**The high value of personal data drives a thriving black market for cybercriminals tools, expertise and data theft.**

ipswitch

Since 2013 , global
**data breaches**
have accounted for
**5.8 billion lost data records.**

Source: Breach Level Index

While no industry that collects and stores personal data is safe, sources such as the Breach Level Index report that 80% of the breaches occur in the technology, retail, financial and healthcare sectors. If your organization collects, stores, shares, processes or transmits personal data, you are a likely target for attack.

Much of the stolen data makes its way to a black market in which prices vary by data type and age (how long ago it was stolen). For instance, per record prices for passwords may be .10 to .20 Euro whereas recently stolen credit cards can be worth from 30 to 50 Euros.

**If your organization collects or processes the personal data of EU residents, regardless of whether or not you have a physical presence in the EU, you are subject to the GDPR.** Under the GDPR, the loss of data due to a lack of adequate policies and protection measures can result in fines up to 4% of corporate annual worldwide turnover.

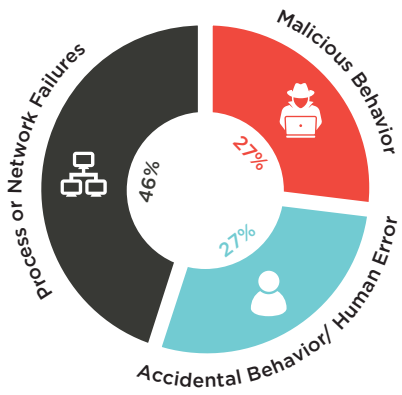
## The Enemy

Who is responsible for data breaches and theft? While the media would have us believe that the predominant cause of our problems is nation states and cybercriminals, the truth is much less convenient. A recent Ipswitch survey of 255 IT professionals showed that only 27% of data breaches are the result of "Malicious Behavior". An equal percentage was blamed on "Accidental Behavior or Human Error". A staggering 46% of all data breaches were caused by "Process or Network Failures". We've met the enemy and they are us.

The truth is that most data is lost because someone within the organization or within a partner organization does something they shouldn't. This may be transmitting data through unsecured means like email attachments or consumer grade web services, or falling victim to a social engineering attack through email or social media.

Sure there are those cases where large numbers of records are stolen through advanced persistent threats from cybercriminals, but, even then, part of their attack chain usually involves the unintended participation of employees or partners.

**Causes of Data Breaches**




## Your Risk Exposure

The GDPR defines 'controllers' and 'processors' as two different types of organizations to which the regulation applies. The controller defines the how and why of personal data processing and the processor acts on the controller's behalf. For instance, if you are a bank that outsources check imaging processes for your on-line customer portal, the outsourcer is a processor.

The GDPR places specific legal obligations on processors including the need to maintain an audit trail of processing activities. Under the GDPR, processors have significantly more liability for a data breach than under the Data Protection Directive.

If you are a controller, the GDPR places more obligations on you to assure that processors are in compliance. You are not relieved of your data protection obligations if a breach occurs in a processors network.

ipswitch

In a recent email spoofing attack, employees of a healthcare organization were asked to respond with their EFSS user names and passwords – **60% complied.**

This is an important consideration when it comes to the application of security policies in the transfer of personal data between controllers and processors. Not only must the transfer be secure, but the data must be protected while it is being processed. In certain cases the GDPR can also be interpreted to state that once the processing is complete, the processor must delete any personal data that is no longer needed.

The first step in assessing your readiness for compliance with the GDPR should be to assess your exposure to the risk of data loss through both controlled and ad-hoc data exchanges with external parties. The three areas to examine are:

- The security of your core business file transfer processes;
- The risk of ad-hoc employee transmissions of personal data via email attachments; and
- The prevalence/security of cloud-based file transmission.

## CORE BUSINESS FILE TRANSFER PROCESSES

Most likely your core file transfer processes, especially those involving personal data, are already centralized to a small group of highly secured FTP servers. Hopefully, these use SFTP or FTPS which leverage SSH or SSL to assure encrypted transmission and authentication. If this is not the case, your troubles may be too large to be addressed by this whitepaper but you should definitely read on.

If this is the case, you should know that even secure file transfer processes (SFTP/FTPS) have limitations that expose you to an increased risk of security breaches and non-compliance. Key components often missing in "best-practice criteria" include automation, visibility, secure tamper-evident logging and non-repudiation.

IT organizations should pay particular attention to the use of unsecured file share technologies such as unencrypted FTP, email, and consumer-grade cloud services by employees and external partners

Security/Compliance Risks of FTP include:

- **Lack of Encryption:** If the server is not SFTP or FTPS capable, file transmissions are in plain text (unencrypted) and vulnerable to theft in transit through a number of easy to use technologies. Exposure of plain-text personal data to the public internet will undoubtedly be a serious violation of the GDPR.
- **Lack of Automation:** Repetitive file transfer requirements are a cumbersome process in most FTP environments leaving organizations exposed to the risk of human error resulting in data loss. Automation of file transfer workflows provides a governance mechanism to mitigates the risk of data loss and non-compliance fines.
- **Lack of Visibility:** FTP servers lack the degree of visibility and logging required for compliance certification. The logs should be tamper-evident and keep track of when a file was transferred, if it was received by the right party, and whether or not it was subsequently deleted.
- **Lack of Scale:** Organizations often rely on IT to develop a collection of home-grown scripts to automate their file transfer activities. As the needs of the organization grow, the scale and complexity of maintaining of these scripts become unwieldy and can introduce unanticipated security gaps.

ipswitch

### AD-HOC FILE TRANSFERS AND CLOUD-BASED TRANSMISSIONS

To ensure compliance with data protection regulations, your organization should implement and monitor adherence to processes that assure the safe handling of personal data. A particular vulnerability is the likelihood that an employee will transmit regulated data via an unsecured means such as an email attachment or a consumer-grade, cloud-based file share service.

**Security/Compliance Risks of Email and Cloud-Based File Share**

- **Encryption:** Files are not likely to be encrypted on the users desktop or in transit.
- **Distribution:** There is no guarantee that transmitted data is received by, and only by, the intended recipient.
- **Data Life:** Files may not be deleted from the mail server or cloud repository and data may continue to be exposed months after the initial exchange.

## File Transfer Security Controls

In the end, data protection becomes a matter of governance, policy enforcement and the implementation of specific security requirements. The ISO/IEC 27001 international standard has been widely accepted as the best-practice reference for security requirements by regulatory bodies across the world. It will undoubtedly be influential in determining GDPR compliance certifications. The table below highlights seven of the ISO/IEC 27001 best-practice controls that are the most pertinent to external file transfer operations.

| Security Requirement | ISO 27001 | GDPR/DPD | File Transfer Control |
|---|---|---|---|
| 1. Compliance | A.18 | Yes | Automation |
| 2. Communications Security | A.13 | Yes | Control & Visibility |
| 3. Information Security Policies | A.5 | Yes | Information Security |
| 4. Access Control | A.9 | Yes | Authentication |
| 5. Cryptography | A.10 | Yes | Cryptography |
| 6. Physical & Environmental Security | A.11 | Yes | Secure Architecture |
| 7. Business Continuity Security | A.17 | Yes | Failover |

ipswitch

1

## AUTOMATION

Commonly used file transfer workflows should be automated to mitigate against the introduction of human error that might result in data loss. Your file transfer tools should support functions such as automatic forwarding, error correction, and confirmation of receipt for all data transfers.

2

## CONTROL AND VISIBILITY

Control and visibility of data flows and events are the most important requirements for effective security management, and essential for validating compliance. Your tools should enable central visibility, control and prior authorization of all file transfers. Logs should be kept in a tamper-evident database to assure the integrity of audit trails.

3

## INFORMATION SECURITY

Your technology, tools or processes should ensure file integrity checks, data deletion after receipt, and non-repudiation (the sender and receiver are both authorized and authenticated to access the data). An important aspect of compliance is the existence of a tamper-evident audit trail that tracks integrity, delivery, authentication, non-repudiation and subsequent deletion of externally transmitted data files.

4

## AUTHENTICATION

The authentication of users and administrators is an essential aspect of security and compliance. Your file transfer systems should be capable of accommodating an array of access control mechanisms, including integration with central user directories, role-based access control and single sign-on as well as multi-factor authentication.

5

## CRYPTOGRAPHY

Encryption algorithms have a limited shelf life. Compliance standards often do not allow the use of compromised systems. It is essential therefore your data sharing systems employ strong, state-of-the-art cryptographic mechanisms and enable secure selection, distribution and protection of encryption keys. To safeguard against future strengthening of data protection regulations, your systems should ensure the continuous protection and integrity of data both in transit and at rest.

6

## SECURE ARCHITECTURE

Your systems architecture should integrate with existing security infrastructures and applications. The systems should also either ensure that there is no unencrypted data within the DMZ or provide for DMZ termination of inbound requests for authentication and data transfer with a gateway proxy server.

ipswitch

7

## FAILOVER

A key requirement of many data protection regulations is secure business continuity. This requirement is meant to safeguard the confidentiality, integrity and availability of file transfers, at all stages throughout any failures, disasters or outages. Automatic, secure failover is essential to ensure that file transfers are either successful or continuously restarted until complete.

# Ipswitch® MOVEit Compliance Features

MOVEit® is a Managed File Transfer system that lets you manage, view, secure, and control the exchange of sensitive data with external parties to assure compliance with data protection regulations. The table below shows how MOVEit addresses each of the seven core best-practices for compliance with data protection regulations.

| Security Requirement | MOVEit Control |
|---|---|
| Compliance | MOVEit helps ensure that file transfers are secured, data is protected at all times, and records of transfers are secured in tamper-proof audit trails for legally required periods prior to assured destruction. |
| Communications Security | MOVEit enables central visibility, control and prior authorization of all file transfers, as well as encryption, traceability and non-repudiation of transfers, including secure audit trails of significant events. MOVEit is architected to integrate with existing security infrastructure, policies, and applications, ensuring there is no unencrypted data in the DMZ and eliminating any requirement for external access. |
| Information Security Policies | MOVEit encrypts files at rest and in transit, provides non-repudiation and file integrity checks. Ipswitch provides email, web, mobile access and desktop clients which, when used with MOVEit provide compliant file transfer access to all users. |
| Access Control | MOVEit offers a choice of authentication mechanisms, including integrations with existing systems, and a rich set of features to support user access management, including blacklists and whitelists, and tools to help administrators select the most appropriate settings to meet security policies. |
| Cryptography | MOVEit employs strong cryptographic mechanisms and secure selection, distribution and protection of encryption and decryption keys, consistent with international legal and regulatory requirements. |
| Physical & Environmental Security | MOVEit's architecture provides flexibility in implementation to ensure adherance to your organizations physical security requirements. |
| Business Continuity Security | MOVEit safeguards the confidentiality, integrity and availability of file transfers at all stages throughout any failures, disasters or outages. Ipswitch Failover can assure uninterrupted file transfer processing. |

## About Ipswitch

Ipswitch helps solve complex IT problems with simple solutions. The company's software is trusted by millions of people worldwide to transfer files between systems, business partners and customers; and to monitor networks, applications and servers. Ipswitch was founded in 1991 and is based in Lexington, Massachusetts with offices throughout the U.S., Europe and Asia.

For more information, visit **www.ipswitch.com**.


### Frost & Sullivan has awarded Ipswitch MOVEit their 2016 Secure File Transfer Product Leadership Award.

In the course of their industry Best Practices Research, MOVEit was found to best address the key customer and industry needs of security, flexibility and scalability while ensuring an unrivaled customer experience and ease-of-use.

ipswitch

Ask Us About a 30-Day FREE TRIAL of Ipswitch MOVEit ›