GDPR-compliant data transfer and file sharing

A WHITE PAPER FROM PRO2COL: THE UK'S INDEPENDENT FILE TRANSFER SPECIALISTS

OCTOBER 2017

pro2col
the file transfer experts

Contents

Introduction to GDPR

This White Paper specifically addresses file transfer in the context of General Data Protection Regulation (GDPR). It is an essential read for organisations wanting to review their data transfer and file sharing systems and processes to make sure they comply with GDPR. File transfer systems include Managed File Transfer (MFT) and Electronic File Sync and Share (EFSS):

- MFT solutions allow data to be transferred securely in a controlled fashion, both inside and outside an organisation, between systems and / or users. Files are transferred more quickly and securely, enhancing productivity and providing visibility of transfers.
- An EFSS system allows users to synchronise and share documents across multiple devices and organisational boundaries.

This White Paper is written by Pro2col, who are independent experts in the file transfer industry and have been for over 14 years. It contains GDPR analysis and recommendations from Pro2col technical consultants.

What is GDPR?

GDPR is a new EU regulation (2016/679) coming into effect on 25 May 2018. It is a stringent set of security measures relating to how and where personal data is collected, handled and used. At its heart, GDPR is about reinforcing individuals' rights. Once in force, individuals will give their consent to how their data can be used, can request to have data deleted, see what data is held about them, or even have their data transferred to another organisation.

Through these new, higher standards of data protection, individuals will take back control. It is hoped GDPR will restore confidence and strengthen the EU internal market, whilst simultaneously providing a consistent framework for implementation and enforcement. GDPR transcends existing data protection legislation. Compliance is mandatory for any EU or EEA member state, plus any organisation holding or using data about any citizen from an EU or EEA member state.

Brexit makes no difference when it comes to GDPR. Britain will still be part of the EU when GDPR comes into effect and therefore needs to comply. The UK Government will implement an equivalent regulation post-Brexit. In addition, organisations holding or using data about any citizen from an EU or EEA member state will need to comply.

Failure to comply will have serious consequences. Fines for the most serious breaches could reach €20 million or 4% of the organisation's Global Annual Turnover, whichever is greater. No organisation – whether an SME, a sole trader, or a multinational – is immune.

The Information Commissioner's Office (ICO) is the UK's independent body set up to uphold information rights. They have stated that they are taking a tough stance when it comes to the GDPR deadline and compliance. In her speech 'GDPR and accountability', Information Commissioner Elizabeth Denham said: "Last year we issued more than one million pounds in fines for breaches of the Data Protection Act, so it's not a power we're afraid to use." She continued: "If a business can't show that good data protection is a cornerstone of their practices, they're leaving themselves open to a fine or other enforcement action that could damage bank balance or business reputation."[1]

[1] Elizabeth Denham, 2017, 'GDPR and accountability', London, 17 January 2017.

GDPR contains 99 separate articles, covering all aspects of data protection. Data Protection Officers will need to review file transfer systems, call systems, anti-virus systems, data classification and data loss prevention systems, policies and training.

What is personal data?

Personal data means any data that makes a living person identifiable. This could be 'direct', such as their name, or 'indirect'. This is where combined information could identify the person. GDPR also refers to special categories, or sensitive data. This includes information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, details of health, sex life or sexual orientation, email addresses and IP addresses. It also includes genetic data or biometric data for the purpose of identifying someone.

Some types of organisation naturally spring to mind when considering personal data. Any medical information or bank details, for example, would be considered highly sensitive. But there are numerous other forms of personal data being transferred within and beyond organisations all the time. For example, data held by finance and accounting departments, including pay slips; legal departments files; and lead information within the sales team. These are just some examples of everyday data that needs to be considered within the context of GDPR.

Organisations must ask themselves whether the data being transferred could be used to identify the individual. Think about the sensitivity of the data and the impact a breach would have on the data subjects and whether the transfer is necessary.

GDPR and file transfer

Reviewing your data transfer and file sharing processes and systems should be one of your first steps towards GDPR compliance. Systems are quick to implement and can address several GDPR requirements simultaneously. Many organisations are unaware though of just how much data transfer and file sharing takes place.

In the digital economy over a third of all business-critical processes involve data transfers. In fact, it is highly unlikely for a business not to be transferring files containing personal data in some way. Digital data can enter and leave a company from a wide range of different sources. This can be in the form of email content and attachments, online forms, uploads to your file transfer servers, collections from supplier's systems, links provided to cloud-based tools, USBs, scripting, out of support software, among others. Fig. 1 shows the wide range of data transfer and file sharing that takes place, all of which needs to be taken into account when assessing GDPR compliance.

Common data transfer and file sharing practices

Fig. 1: Common data transfer and file sharing practices

Unmanaged in-house scripts

In-house scripts in particular are one of the biggest risks to an organisation's GDPR compliance. They are commonly used in organisations to move data between systems and Pro2col file transfer experts believe they will almost certainly not comply with GDPR. They lack central visibility and audit trails, have single points of failure and no change control. In-house scripts often have poor or non-existent error handling and performance issues. Passwords are typically stored in plain text so it's difficult to enforce security and encryption.

Compliant data transfer and file sharing

Figure 2 outlines the six key areas where GDPR impacts data transfer and file sharing. This references the relevant article from the regulation, alongside recommendations for compliance. This is followed by a detailed description of the recommended file transfer features that will address the requirement.

GDPR requirement	Recommendations
Consent In article 4, GDPR defines consent of the data subject as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her." Although a file transfer system is not the place to manage consent for how data is used (eg: marketing purposes), it must be able to manage consent for how data is used **within the system**. Simply creating a user account for someone to access the file transfer system requires that user's consent. This means that whenever organisations create a user record with any identifying characteristic in their file transfer system, the user must provide consent for you to store the information. This is still the case even if it is just a temporary record. Organisations must present a clear explanation of what they will do with the data and the user must acknowledge agreement. An opt-out clause is not acceptable. Organisations must find a way to store this acceptance and be able to produce the record at any time to demonstrate the user's agreement. Be careful to store the actual content of the consent message in order to prove that it has not changed since the time of signing.	A consent message should explain exactly what the organisation will do with the user's data record. An example can be seen in appendix 1.

Storage and accessibility Article 25 focuses on 'Data Protection by design and default'. This is about embedding data protection into business processes, systems and services from the outset; not as an afterthought. Article 25 states organisations have an obligation to 'implement appropriate technical and organisational measures' to protect personal data. This specifically mentions 'storage and accessibility'. It goes on to say: "Such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons."	This means access to personal data should be restricted to only those people that have a necessary and justifiable business need. Features meeting these requirements include: • Authentication / access control • Storage Retention and availability • Encryption at rest
Record of processing activities Article 30 focuses on 'Record of processing activities'. It states that organisations must 'maintain a record of processing activities'. This means organisations should have a log showing all personal data transfers that occur. This information should be available, alongside the impact assessments (see below), as evidence that the transfer has been completed securely. This includes 'recipients in third countries or international organisations.'	Features meeting these requirements include: • Reporting • Impact assessments • Retention period • Geographic visualisation of transfer
Security of processing Article 32 focuses on 'Security of processing'. It states that organisations must 'ensure a level of security appropriate to the risk'. This article outlines the requirement for 'encryption of personal data' and 'the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services'. Regular testing will expose any vulnerabilities that an attacker could exploit. Article 32 outlines the testing requirement as 'a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.'	This means organisations must have sufficient security measures in place for transfers. They should also carry out regular scheduled audit reports and regular penetration testing against file transfer systems. Features meeting these requirements include: • Auditing • Penetration Testing • Encryption at rest/in transit • HA/DR (RTO) availability • Pseudonymisation / anonymisation • Approval to process • Access control

Data Protection Impact Assessment (DPIA) Article 35 outlines the requirement for a DPIA. This is there to ensure organisations are giving due consideration to the nature of the data they are transferring, the risks associated with it, and the measures in place to mitigate them. The DPIA is a document that describes the nature of the data, the purpose of the transfer, how it is performed and the security configuration. A DPIA is required for all data transfers and file sharing. The higher the risk identified in the DPIA the greater the protection must be. The DPIA must be carried out in advance of the transfer and all data transfers must be carried out in line with this document and audited against it.	The DPIA is an external document detailing transfers. A list of example questions can be found in Appendix 2. Some file transfer systems have the ability to build impact assessments within the software, simplifying this requirement.
Availability of data GDPR makes several requirements for data availability: Articles 15, 17 and 20 refer to particular individual rights: Article 15 explains the 'right of access', where individuals can request access to all personal data an organisation holds about them; Article 17 refers to their 'right to erasure', where organisation must erase all personal data 'without undue delay'; Article 20 outlines individuals' 'right to data portability', which means transferring personal data to another system or company. Article 32(1)c states organisations must have the 'ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident'. This means organisations who are reliant on a single server could find themselves in breach of GDPR.	Features making this requirement easier include: • Storage Retention and availability • HA/DR (RTO) availability

Figure 2: Key areas where GDPR impacts data transfer and file sharing.

Features aiding compliance

- **Encrypted at rest (e.g. PGP, AES)**
  This is achieved by encrypting either individual files or entire file systems. When a file system is encrypted, it is generally using technology like Bitlocker. For individual files an application may use proprietary encryption techniques like AES256, or else employ an encryption/decryption tool (for example PGP or GPG).

- **Encrypted in transit (e.g. SFTP, FTPS, HTTPS)**
  Transit encryption requires channels passing the commands and data to be encrypted, regardless of whether the files being transmitted have already been encrypted. FTPS and HTTPS uses SSL encryption, which has certificates to prove the identity of the receiving server. The actual encryption occurs based upon a unique key inside the certificate. SFTP uses SSH to encrypt the channel, and – similar to SSL – the channel is encrypted based upon the receiving server's public key.

- **Authentication / Access Control**
  Organisations should be able to create unique user identities within a file transfer system, and monitor user activities. The system either needs to provide a robust mechanism for setting password strengths and expiration policies, or use existing security systems to manage these (these are generally more advanced). Some systems offer Multi Factor Authentication (MFA), where users have to confirm their identity by another means (eg: Entering a unique code sent by email or text). Additionally, the system should restrict users to only access the data they require, whilst not being so restrictive that they cannot work. Organisations also need to think about how third parties authenticate their identity. For example, a recipient at another organisation should authenticate their identify when receiving files through an EFSS system.

- **High Availability / Resilience**
  Modern file transfer systems are generally configured in a way that allows their services to continue, following the critical failure of one or more components. This may be managed by a highly available infrastructure – with minimal or zero downtime achieved by load balancing and removing single points of failure – or by restoring a system to a standby server and recovering to a previously agreed time (Recovery Point).

- **Reporting**
  As outlined in figure 2, it is important to keep a record of all transactions performed by a file transfer system. Some systems will provide this in great detail, others not so much. In either event, it is preferable to have a reporting process built into the system for both ease of use and transparency.

- **Storage Retention**
  One of the biggest issues with any file transfer system is the tendency to have an abundance of old files remaining in it. This often comes from user's reluctance to delete files following their download. As a consequence, old forgotten files containing confidential data may be left around even though there is no requirement for them. To address this, some file transfer systems contain housekeeping routines to clean old files after they have been downloaded or a suitable period has passed. It is imperative that these housekeeping rules are applied and adhered to.

- **Pass GDPR Audit**
  File transfer systems need to be tested periodically to ensure that their security is still in place and adequate to the task. Some file transfer systems have preconfigured reports that can be executed to demonstrate this, while others will rely on auditor reviewing system configuration. Additionally, as file transfer systems are frequently internet facing, external penetration tests need to be performed to ensure that they do indeed meet security criteria.

Common compliance fails

Figure 3 indicates how many of the most common file transfer activities do not meet GDPR requirements. The cross indicates a definitive non-compliance and the tick indicates compliance. The question mark indicates that some may comply, or partially comply.

	Encrypted at rest (e.g. PGP, AES)	Encrypted in transit (e.g. SFTP, FTPS, HTTPS)	Authentication / access control	Consent to store and process data	High Availability / Resilience	Reporting	Storage retention	Pass GDPR audit
Email Attachment	X	X	X	X	?	?	X	X
FTP (open source)	X	?	?	X	X	?	?	X
Scripting	?	?	?	X	X	X	?	X
Consumer SaaS*	?	?	?	?	✓	?	✓	X
Microsoft IIS	X	?	✓	X	X	X	X	X
USB/DVD	?	?	X	X	X	X	X	X
Out of support software	?	?	?	?	X	?	?	X
Customer systems	?	?	?	?	?	?	?	X

Figure 3: Common file transfer activities do not meet GDPR requirements.

**Could include services like WeTransfer, Hightail, Google Drive, OneDrive, Dropbox personal edition.*

Recommendations

Many organisations will have decades worth of stored personal data that will eventually need to be reviewed under GDPR. Sorting through this could take months. The most important first step an organisation can take is to implement GDPR-compliant file transfer from now. This means reviewing data flows, identifying weaknesses, identifying tools or procedures that need to be put in place to fix them and then putting the new procedures and tools in place.

Organisations are most likely to be at one of two points in their journey towards GDPR compliance.

No secure data transfer or file sharing systems in place

Organisations without file transfer procedures, policies or systems are at greatest risk of a data breach. It is likely these organisations are relying on the insecure practices outlined in figure 3. They will need to conduct a thorough review of the kinds of transfers required and which fall under GDPR. Each transfer will require an impact assessment and then the correct technology put in place to meet the requirements.

- Pro2col's GDPR Advisory Service offers a pre-implementation planning option. Pro2col technicians review data transfers and identify which fall under GDPR. They assist in creating impact assessments and planning technology and interface configuration.
  More information and pricing is available from the 'Plan' section of pro2col.com or by calling +44 (0)20 7118 9640.

Some organisations may also require a more thorough requirements analysis. This means scoping current and future data transfer and file sharing requirements for all stakeholders within the business, and identifying a file transfer solution that meets those needs. It is important to do this process thoroughly, because sourcing the wrong solution will cost more money in the long run.

- Pro2col offers a Needs Analysis service. An experienced expert will go through over 230 questions, fully scoping the organisation's requirements. This includes current and future needs of all the stakeholders in the business, plus any technologies that need to be integrated. Clients receive a comprehensive review and a recommendation. More information is available in the 'Plan' section of pro2col.com or by calling +44 (0)20 7118 9640.

Checking GDPR compliance for existing systems

Organisations who already have data transfer and file sharing systems in place will need to identify which fall under GDPR. Each transfer will require an impact assessment of the relevant interfaces checked.

- Pro2col's GDPR Advisory Service offers a post-implementation planning option. Pro2col technicians identify which existing interfaces require GDPR compliance, assist in gathering information relevant to each transfer and documenting the interfaces. They will support organisations creating their impact assessments too. Where interfaces do not comply with GDPR, they will make remedial recommendations. More information and pricing is available from the 'Plan' section of pro2col.com or by calling +44 (0)20 7118 9640.

About Pro2col

Pro2col are independent experts in the file transfer industry and have been for over 14 years. Pro2col technical consultants have delivered over 750 solutions across the globe, for a wide range of industry sectors and use-cases. Clients include KPMG, Red Bull Racing and John Lewis. Pro2col technical consultants advise organisations through the different stages of their file transfer project to make sure it is a success. Whether that is scoping requirements, product demos and proof of concept / software evaluations, negotiating the best deal with vendors or installations and training, find out more on the Pro2col website or speak to an expert on +44 (0)207 118 9640.

Appendix 1: Example consent message

The example consent message can be used either as a form where the user clicks to confirm consent, or as an email where the user replies giving their consent.

Example consent message

It is important that you read this information about how we will process your personal information, before giving your consent.

We will use your name, email address and phone number to uniquely identify you as a user of our Managed File Transfer system. This is the sole purpose that we will use this information for. You may periodically receive communications from us pertaining to your use of our Managed File Transfer system.

Your account may be removed by us at any time either as part of an internal process or at your request. In either case, a record of your activity on our Managed File Transfer system will be retained for historical research purposes.

Your personal data will never be shared with another organisation.

If there is any change to any of these statements, we will contact you and seek your consent again.

Please click the acknowledgement button / reply to this email below [delete as appropriate] giving your consent.

Appendix 2: Impact assessment questions

Whilst impact assessments will vary across organisations and departments, some questions one might expect to see with regard to the transfer of data include:

- Who are the stakeholders?
- Do the files contain personal data?
- If so, which categories of personal data and what is the sensitivity level?
- How many data subjects does each file contain data for on average?
- Where is the data being sent? Within the EEA, outside of the EEA, is it covered by standard contractual clauses, model contracts, Binding Corporate Rules etc.
- What is the reason for this transfer?
- Is this transfer required for lawful legitimate business purposes?
- Is this transfer aligned with the consent of the data subject if required?
- Who will have access to this data?
- What is the overall risk category based on the above?
- What data protection measures can be applied to mitigate the risk of a data breach:
    - Transfer using secure transfer protocols only
    - Encrypt data at rest and in transit
    - Minimisation of data
    - Anonymise personal identifiers
    - Pseudonymise personal identifiers
    - Ensure transfer is authorised by the relevant personnel prior to going live
- Sign-off of the transfer requirement