

FILE TRANSFER AND THE GDPR

File Transfer Features Needed for GDPR Compliance

The General Data Protection Regulation (GDPR) encompasses 7 data protection principles that, together, assure the rights of the individual are central to the collection and processing of personal data.

File Transfer systems, fitting the definition of ‘processing’, **must provide the following functionality in order to enable compliance.**

“ ” THE 7 GDPR DATA PROTECTION PRINCIPLES

GDPR-REQUIRED FILE TRANSFER FUNCTIONALITY ✓

PRINCIPLE 1

“Fair, lawful and transparent processing”

Additional care must be used when designing and implementing personal information processing activities.



- ✓ **Non-repudiation** to validate that personal data is transferred only between authorised senders and receivers.
- ✓ Centralised, fine grained **access control** to safeguard user credentials, permissions and personal data.

PRINCIPLE 2

“Data Security”

Personal data must be secured against internal and external threats, accidental loss, destruction and damage.



- ✓ **Encryption** of personal data in transit and at rest.
- ✓ Integration with **Data Loss Prevention** and **Anti-virus** solutions.

PRINCIPLE 3

“Accuracy”

All reasonable steps must be taken to ensure that personal data is accurate.



- ✓ **Automatic file integrity checking** to validate that a file has not been altered.

PRINCIPLE 4

“Accountability”

Compliance with the Data Protection Principles must be documented.



- ✓ Automatic **collection** and reporting on data transfer logs on one centralised consolidated location.
- ✓ Audit logs should be **tamper-evident** in order to be trusted for accuracy.

PRINCIPLE 5

“Purpose Limitation”

Personal data collected for one purpose should not be used for a new incompatible purpose.



- ✓ Cryptic scripts should be replaced with a **forms-based solution** that provides a standardised, secure and documented record of data transfer tasks.

PRINCIPLE 6

“Data Minimisation”

Collection and processing should be limited to the personal data needed to achieve the stated purpose.



- ✓ **Comprehensive analytics** that provide the required insights into transfer activities to assure on-going compliance with GDPR’s data protection principles.

PRINCIPLE 7

“Retention Periods”

Personal data should not be retained longer than needed for the stated purpose.



- ✓ The system should allow the **scheduling of common repetitive pre- and post-transfer tasks**, including the scheduled deletion of personal data files.



The lowest risk, most cost-effective way to meet all 7 GDPR Data Protection Principles is a managed data transfer solution like Ipswitch MOVEit File Transfer.

MOVEit integrates secure data transfer with centralised workflows, access control, and audit logging. 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. Learn more by trying a

▶ FREE TRIAL OF MOVEit MANAGED FILE TRANSFER ◀