FILETRAIL

GDPR Intersects with Information Governance

Law firms are facing the challenges and threats of GDPR this May. GDPR is the largest change to data protection legislation in 20 years and gives regulators unprecedented power to impose fines on companies conducting business in Europe.

Implementation of a GDPR programme across a law firm's information governance system can only be scaled with automation. FileTrail's information governance software and project methodology are designed to go beyond GDPR compliance, ensuring organisations are prepared to meet its stringent requirements.

FileTrail offers:

- Synchronisation
- Centralized Auditing
- Granular Authorisation
- Authority synchronization
- Content Lifecycle Management
- Policy Management

3 WAYS FILETRAIL HELPS WITH GDPR COMPLIANCE

FileTrail's information governance software, Governance Policy Suite (GPS), ensures organisations can meet several key operational requirements mandated by GDPR.

1 RIGHTS OF INDIVIDUALS

Right of access

FileTrail supports compliance with the subject's right to access information (Article 15). All PII data is tied to a singular entity instance in the database. All apparent occurrences in the UI are actually references to the singular instance. This makes is easy to access the information, with the assurance that it is the only copy or variation of the data.

Right to be forgotten

FileTrail supports the right to be forgotten and de-identifying through anonymisation (Article 17). All PII data is tied to a singular entity instance in the database. All apparent occurrences in the UI are actually references to the singular instance. FileTrail synchronizes user profiles and data fields from authority systems, such as Active Directory (AD) and financial systems (such as Aderant and Elite) . When a controller implements anonymisation or pseudonymisation in these sources, it is automatically reflected in FileTrail.

2 ACCOUNTABILITY

Data Access Management

FileTrail supports restrictions on access to fields containing PII (Article 24). Our comprehensive and granular security allows you to control access down to the field level, specifying what users or groups have rights to view or edit each field.

Data Processor Accountability

FileTrail provides accountability of data controllers involving the subject's information (Article 30). FileTrail logs all activities – including adding and editing, transactions, and more – tying each to the data controller, the user of the system. FileTrail also surfaces those activities through audit trails in the UI and through audit reports.

3 DATA PRIVACY AND PROTECTION

Data Protection by Design

FileTrail was built with protection by design and by default (Article 25). FileTrail allows the controller to implement data protection measures, including anonymisation, pseudonymisation, and data minimization. Our user-defined fields enables the controller to define and store only the personal data which is necessary for the purposes for which FileTrail is used. FileTrail also provides the mechanisms for the controller to demonstrate compliance. The UI includes easy access to personal data and security controls, where viewing and editing rights can be restricted. And detailed audit trails and audit reporting tools are included.

Information Security

FileTrail provides technical measures for information security (Article 32). Our comprehensive and granular security allows you to restrict and ensure appropriate access to PII with granular controls over who can view or modify data both broadly (e.g., by Practice Area or Administrative Department) and granularly down to the field level, specifying what users or groups have rights to view or edit each field.

HOW FILETRAIL HELPS WITH GDPR PROGRAMMES

Developing a plan to comply with new GDPR rules is critical for all organisations. By design, FileTrail's software and project methodology support organisational GDPR planning and strategy. In many cases, FileTrail even makes your GDPR programme run more smoothly. Here's how we can help:

STRATEGY AND GOVERNANCE

When considering strategy and governance in your GDPR program organisations must define an overarching privacy programme governance structure, and create roles and responsibilities for coordinating, operating, and maintaining the programme on an ongoing basis.

FileTrail's methodology helps organisations define roles and responsibilities for maintaining and reporting GDPR compliance. FileTrail also synchronizes roles and responsibilities, as well as data (from AD, Matter Intake and financial systems), eliminating the need for manual administration in FileTrail.

FileTrail's automated synchronisation can be set-up to include flags from financial systems (such as those indicating a Matter contains PII or PHI) and security settings (that control who may see Matter data and Items related to a Matter). The Matter data fields that hold the flags for PII or PHI are searchable and reportable. This provides quick access to all qualifying Matters (active, closed or both), through FileTrail's MasterList Search tool and the Search Results Download tool.

'... organisations do not need to undertake additional efforts to manage the data lifecycle in FileTrail.'

DATA LIFECYCLE MANAGEMENT

GDPR compliance requires data lifecycle management. As defined by Gartner, this is "the process of managing business information throughout its lifecycle, from requirements through retirement….[crossing] different application systems, databases and storage media. The cycle is made up of phases of activity including create, use, share, update, archive, store and dispose."

In order to minimize data, FileTrail's project methodology includes a period during which we guide you through defining fields for PII, making sure to include only those fields which are necessary for the process performed by FileTrail. This way, synchronization of data from authority systems – such as AD, HR systems, or financial systems – will only include the minimal data required. Keep in mind that any anonymisation or pseudonymisation performed in authority systems are automatically synchronized into FileTrail. This ensures organisations do not need to undertake additional efforts to manage the data lifecycle in FileTrail.

POLICY MANAGEMENT

When designing and implementing a program, organisations should consider that GDPR compliance requires privacy policies, notices, procedures and guidelines be formally documented and be consistent with applicable laws and regulations.

FileTrail's approach to data architecture ensures that privacy policies are easily applied. Access to the singular copy of PII is easy, while restriction of access is provided by a comprehensive and granular security system. Anonymisation or pseudonymisation are supported through automated synchronisation with authority systems (AD for user data, and financial systems for Client and Matter data).

CROSS-BORDER DATA TRANSFER

When creating your GDPR programme, organisations should make sure to create a cross-border data transfer strategy that is based on current and future planned data collection, use, and sharing.

FileTrail accommodates security measures for data in transit and data at rest, including RSA-2048, SHA2, SSL/TLS, IPSec, SSH, S/MIME, OpenPGP/ GnuPG/PGP, and encrypted backups. Specifically, data transmissions are encrypted using 2048-bit SHA-2 encryption (TLS/SSL, HTTPS, FTPS). User passwords are encrypted using a seeded SHA256 one-way hash algorithm (FIPS compliant).

The FileTrail Cloud (Microsoft Azure) is ISO 27001 certified. In addition, a VPN helps provide a secure mechanism for encrypting and encapsulating private network traffic and moving it through an intermediate network. Data is encrypted for confidentiality. Packets that might be intercepted on the shared or public network are indecipherable without the correct encryption keys. Data is also encapsulated, or wrapped, with an IP header containing routing information.

PRIVACY INCIDENT MANAGEMENT

When creating your GDRP Program, organisations should align incident response processes with GDPR specifications and reporting requirements. They also should establish a triage approach to evaluating potential privacy breaches and incidents.

FileTrail's approach to data architecture simplifies incident response. Access the singular copy of PII through our UI is easy. And audit trails and audit reporting ensure you can harvest all activities performed by a user or against PII of the data owner.

TRAINING AND AWARENESS

Training and awareness is important for GDPR programmes. Organisations should make sure to define and implement a training and awareness strategy at both the enterprise and individual levels to ensure GDPR compliance.

All of FileTrail training, documentation, and support videos comprehensively cover tools to secure access to PII and synchronisation of PII data with authority systems (AD for user data, and financial systems for Client and Matter data).

ABOUT FILETRAIL

Since 2000, FileTrail has been developing, implementing and supporting enterprise-class information management solutions.

Deployed all over the world, the company offers a highly configurable suite of records management and governance tools to help organizations manage the complete information lifecycle.

FileTrail is the *only* records management system for law firms, offering both cloud and on-premise solutions. FileTrail integrates with Iron Mountain, Elite, and the Intapp suite. It leverages APIs to apply retention policies and disposition to documents in NetDocuments, iManage, OpenText eDOCS, and other repository-based products.

FILETRAIL

For more information about FileTrail's records management and information governance software, visit

www.filetrail.com.