opentext™

Prepare for GDPR compliance with OpenText™ File Intelligence

Identify and act on content that contains personal data, wherever it resides

The General Data Protection Regulation (GDPR) regulates the collection, storage, use and sharing of personal data. Personal data is defined very broadly under the GDPR as any data that relates to an identified or identifiable natural person. Almost all organizations have such data throughout their organization within vendor databases, employee satisfaction surveys, email content, HR systems, contract and legal systems, reference program records, HR databases and elsewhere. Data that belongs or relates to EU residents must comply with the GDPR. It's important to remember that personal data doesn't need to be stored in the EU to be subject to the GDPR. The GDPR applies to data associated with EU residents even if it is collected, processed or stored outside the EU.

It is important to identify and inventory your organization's content and data to validate which information is affected by the GDPR. Legacy applications and systems often house out-of-date information. Taking inventory of all your data will help you identify the content that contains personal information, the systems that collect and store content and the length of time the content is retained.

Where is personal information hiding?

Potentially regulated data can be hiding anywhere in an organization—on laptops, business applications or file servers, in an old legacy system or AS/400 file share. The employees who originally collected this information may have already left the organization, leaving an unclassified mess and a potentially risky situation.

BENEFITS

- *Deploys quickly, delivering rapid time to value*
- *Identifies content anywhere on your network*
- *Prompts for actions based on type and classification of content*
- *Protects personal information through automated policies*
- *Indexes content and measures risks, providing the information to ensure compliance*
- *Increases efficiency by eliminating manual tasks*

The old concept of security by obscurity no longer applies. The GDPR requires organizations to make reasonable efforts to safeguard all EU resident data. In addition, if users request to remove their data, organizations must be able to ensure that the request is completed.

Easily identify personal information

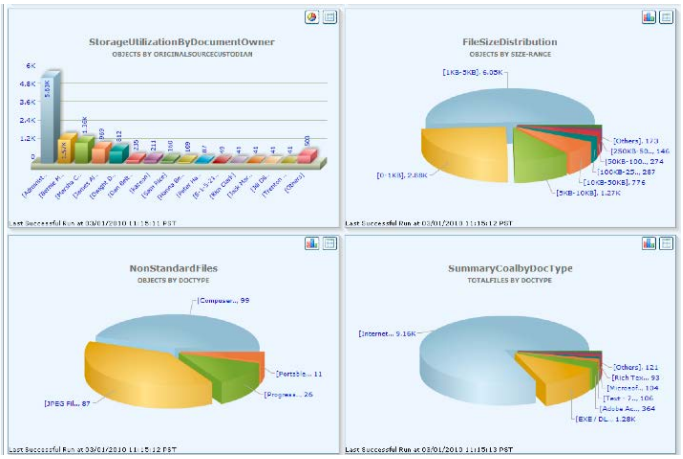
OpenText File Intelligence prepares organizations for GDPR compliance by identifying and managing content in the IT environment that contains personal information. The first step is metadata indexing, which produces a roadmap to uncover characteristics about content, such as its age, last update, author and some personal information. The next step, full text indexing (crawling the text within the files), allows organizations to uncover a greater level of file detail which can be critical for responding to events such as GDPR related data subject requests, regulatory audits or internal investigations and identifying content such as payment card information, national identification numbers, taxpayer IDs or intellectual property. These indexing choices are an important step toward understanding what personal information the organization contains and the business value of the unstructured content—illuminating what is valuable, identifying what may contain risk for the organization and ensuring that the information is retained, protected or disposed of as needed.

Content classification

File Intelligence's classification abilities build on content indexing by categorizing content based on its value. The organization can classify files by attributes (file type, owner, creator, accessed date, modified date) for foundational insight into content's business value. Content can also be classified based on its file content to identify personal information that should be retained or disposed of after use. File Intelligence identifies specific personal information such as payment card information or PII (personally identifiable information like national identification numbers. Classification can also be based on combined metadata or based on user-created or administrator tags. These classifications and subsequent values can be applied to large volumes of similar groups of content. The results can serve as a catalyst for enabling subsequent policy actions and rules. This automated approach results in a quicker time to value and a higher degree of accuracy than the manual approaches organizations may use.

Actionable intelligence with powerful reporting

File Intelligence delivers numerous out-of-the-box reports. With each report category, organizations can create a summary report that aggregates the data in that particular report category, or view a detailed report that includes metadata at the file level about each piece of content that fits the report criteria.



File Intelligence graphical analytics of discovered content

From a GDPR perspective, reports can be utilized to identify and measure levels of risk based on classifications of personal information. Insight from reports can be used to create automated policies and actions such as duplicative file management, defensible document deletion and other regulations and data minimization policies. Automated actions can be set up to protect sensitive, personal and regulated information by moving and retaining the data into a compliant data store such as OpenText™ InfoArchive, OpenText™ Content Suite or OpenText™ Documentum™.

First step to GDPR preparedness

File Intelligence is the first step to assess where personal information challenges lie, what content types are proliferating and determining business value, cost and potential GDPR risk. Being able to quickly deploy File Intelligence, organizations gain rapid time to value—a stark contrast from most governance and compliance projects. File Intelligence's auto-classification capabilities, automated actions and policies allow organizations to prepare for the changes and regulations the GDPR will bring.

www.opentext.com/contact