FILEFLEX TECHNOLOGY

Data Protection Enablement for GDPR Compliance

Cyberithm

A white paper by Cyberithm

qnext

Sponsored by Qnext

FILEFLEX & GDPR COMPLIANCE

This White Paper introduces FileFlex a data collaboration and management platform. With the upcoming requirements of complying with GDPR in 2018, the FileFlex technology supports and augments an organization's compliance endeavors. FileFlex utilizes an organization's existing investment in technology, combined with a rapid deployment capability and with the ability to support enforcement of compliance and the auditability controls required by GDPR. This is achieved while supporting deduplication of data.

The European General Data Protection Regulation (GDPR) requires organizations that not only reside within the EU but also conduct business with the EU to comply with an increased focus on the protection of Personally Identifiable Information (PII) of EU citizens and residents.

The GDPR regulation becomes effective on May 25, 2018. The regulation introduces stiff penalties for non-compliance which may be as high as 4% of total world-wide revenue.

As a binding regulation with focus on the data element it becomes quickly apparent that organizations can no longer blame technology failures as an excuse.

Therefore, organizations that process in-scope EU resident or citizen data are quickly realizing that enforcement of controls around such data is a critical requirement in their arsenal of technology controls.

Moreover, with digital transformation impacting organizations, the ability to maintain control of data is a challenge that organizations are ill equipped to handle where the same data may reside in numerous locations. In parallel, this same transformation is quickly enabling organizations to increase collaboration and productivity.

The control of data transfer is a key requirement of GDPR. First, FileFlex enhances control over data and data transfer by enabling organizations to control and decrease the number of unstructured data copies they require. Second, FileFlex does not have 3rd party dependencies decreasing over-all compliance management requirements. Third, FileFlex provides granular authentication controls over data. Fourth, FileFlex enables access controls in the form of view-only sharing mode where downloading is restricted.

The GDPR's focus on technology is much more prescriptive than its predecessor, the Data Protection Directive. To be effective, however, the GDPR must contribute in the delivery of business transformation

and legal compliance. It does this in several ways. It mandates the use of Privacy by Design techniques and the execution of risk assessments. It also identifies data management techniques such as data mapping and techniques for how to handle operational failure, such as breach disclosure.

In addition, with the looming deadline in May, 2018 organizations that have not implemented effective measures to comply with the regulation must do so promptly. Data controllers and processors who are engaged in the design, build and delivery of GDPR programs should re-examine and rebalance their priorities in order to deliver the best possible technology environment for personal data before the GDPR comes into force in May 2018.

In weighing up the various requirements and associated options, controllers and processors should bear in mind that data protection law delivers incentives for the delivery of technology change. This is in addition to the obvious risks associated with non-compliance which entail risk of regulatory enforcement action, including the risk of sizeable financial penalties. Moreover, there is a new 'litigation risk' built into the GDPR, all underpinned by transparency mechanisms that will shine a spotlight on what is happening to personal data, including when security fails.

Interestingly, the ability to comply with GDPR enables organizations to create the equivalent of a competitive advantage, these benefits are in addition to the obvious gains to be made from taking a 'good' approach to the technology issues.

Advantages such as efficiency and productivity gains are not new to data protection but are also now delivering a stronger focus on data protection in B2B procurement and contractual processes.

Businesses and their contracting partners are starting to ask probing questions and indeed require compliance with the standards they themselves must achieve. This translates into business relationships where the foundational requirement is mutual compliance with the GDPR and in turn organizations that adopt GDPR based approach will perform better in a competitive market.

Likewise, consumers will increasingly factor-in data protection issues when choosing where to conduct their business.

The GDPR's focus on technology is much more prescriptive than its predecessor, the Data

GDPR CHALLENGES

GDPR introduces many operational challenges for organizations that process EU citizen or resident PII. These challenges include:

COMPLEXITY - Unlike technology, which is foundationally structured upon clear rules and requirements, the GDPR is complex and open to interpretation. There is little value to be overly prescriptive as there are typically several ways to achieve a particular outcome, especially where different data and technology is utilized. Technology thrives on certainty, rules and clear requirements, yet the GDPR is both complex and open to interpretation.

FileFlex is a technological control that reduces complexity. The organization's existing infrastructure and existing information security investment and associated controls are utilized to share files while existing identity and access controls such as enterprise active-directory are used to enable authenticated and approved file access. These capabilities enable a rapid deployment model while relying on existing security controls and storage infrastructure to deliver collaboration and file share.

DATA TRANSFER - GDPR requires the enterprise to manage all personally identifiable information (PII) pertaining to EU citizen information and not store or transfer it in or through countries or organizations outside the EU that do not have equivalently strong data protection standards, yet many organizations do not know where all their personal data resides. With the advent of cloud services and cloud based infrastructure services, organizations must now understand where their data is stored. With the typical enterprise utilizing anywhere from tens to hundreds of cloud services, the complexity of understanding where data resides and who has access to the data is growing exponentially. Moreover, GDPR mandates strict breach notification requirements, however, organizations many times do not know where PII data may reside.

FileFlex enables file sharing without the need to duplicate data. Data may remain under corporate security controls or it may be accessed and copied as required. However, detail logging and accounting controls enable organizations to review what the scope of a data access or download entailed. In removing reliance on 3rd party providers FileFlex simplifies compliance and risk management programs and additional built-in controls restricting downloads and view-only mode capabilities provide granular access controls further augment governance, risk and compliance management goals.

GDPR requires the enterprise to control the processing of all personal information, yet the rise of shadow IT takes control away from the IT department and disperses it across the business functions.

FileFlex minimizes the underlying need for Shadow IT existence in the first place, specifically around file sharing and access to unstructured data. Corporate users and external users can share and collaborate under a secure framework and with little need to duplicate data. This in turn, creates a smaller foot-print for attack vectors while enabling the collaboration features users demand.

In addition, FileFlex includes technology, which when used with policies and appropriate user behavior can help protect information, including PII and aid in the prevention of data loss. FileFlex allows IT administrators to restrict sharing to in-company contacts only and users can be prohibited from adding their own contacts. Thus, if configured to do so, FileFlex can be used to restrict sharing so that a sharing transfer of PII outside of the organization is impossible with FileFlex.

GDPR now provides the incentive for business to address data privacy through technology and the technologist needs to understand the range of capabilities that can be deployed to achieve compliance. With the use of FileFlex, infrastructure complexity is reduced and security posture is increased.

GDPR & FILEFLEX – PRIVACY BY DESIGN

With the use of FileFlex in an organization that requires compliance with GDPR the enterprise addresses several key requirements. GDPR requires the use of Privacy by Design techniques which means that enterprises must begin and utilize information security in a "baked-in" approach vs "bolted-on" approach that is prevalent in the industry. GDPR aims to transition information security from an after-thought to fundamental requirements. GDPR also identifies data management techniques, such as data mapping and techniques for how to handle operational failure, such as breach disclosure.

DATA MINIMIZATION

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

This principle should be delivered in the technology stack with the key aspect being the limitation on the amount of data that is in-scope. Utilizing FileFlex technology enables organizations to achieve this goal by significantly reducing the footprint of organization data.

ACCURACY

Personal data shall be accurate and where necessary, kept up to date.

Keeping in-scope PII accurate and up to date is a challenge for organizations as the volume of data grows. FileFlex enables organizations to maintain far less copies of the same data enabling them to keep more accurate and up to date.

STORAGE LIMITATION

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

This principle is further supported by FileFlex software via limiting the number of unstructured data copies that must be maintained, and through the use of audit-

ing capabilities, enabling time limited sharing of files. This aspect in conjunction with view-only mode, supports the protection of PII and aids the prevention of data leakage requirements within GDPR.

INTEGRITY AND CONFIDENTIALITY

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organizational measures.

FileFlex supports integrity and confidentiality of data using technical controls such as LDAP integration, enforcement of file share permissions and support of confidentiality controls by significantly enabling the organization to limit the number of data copies required for collaboration.

ACCOUNTABILITY

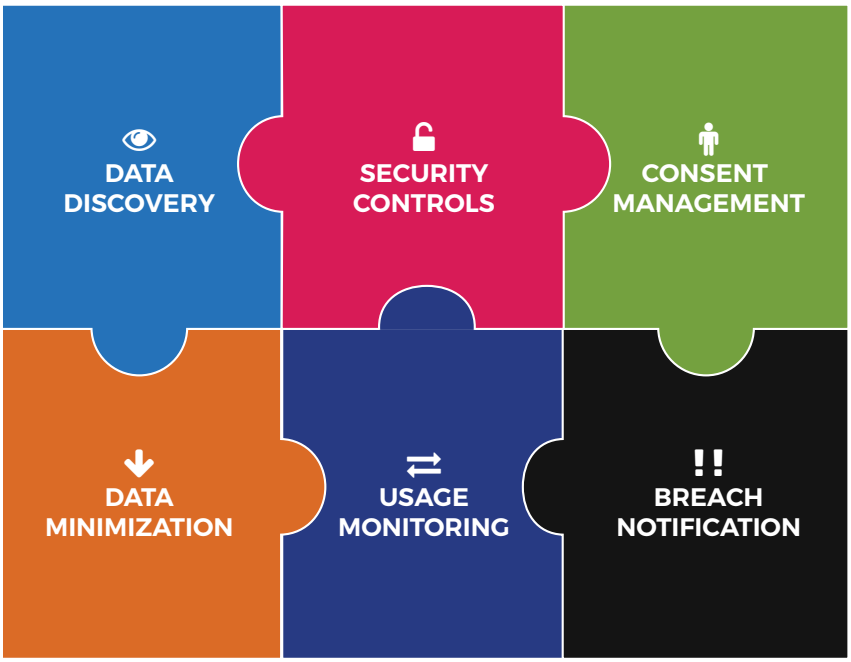
The controller shall be responsible for, and be able to demonstrate compliance with the GDPR.

The extensive logging integration within FileFlex supports this core principle while the integration with LDAP systems such as Active Directory enables controllers to attest to this principle using capabilities that they are already familiar with.

ARTICLE 5 - GDPR CORE PRINCIPLES

GDPR introduces 7 core principles relating to processing of personal data. These principles include: lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability.

FileFlex supports these core principles and can be rapidly deployed in a large enterprise environment to meet the May 25, 2018 timeline.



SUMMARY

In summary, FileFlex supports the GDPR framework by augmenting key requirements such as:

Data transfer – encourages data deduplication and storage of data in source locations within the established security controls of the enterprise. Granular access controls and View-only sharing combined with the ability to restrict contacts are features that when utilized with the appropriate organizational security policies can support data leakage defenses and PII protection. The overall architecture supports smaller more efficient infrastructure to deliver the same services and lessens the reliance on 3rd party services which in turn lessens complexity of compliance management.

Data discovery – using extensive auditing, robust user interface and minimization of data, it is far easier to manage discovery of data and control where data should reside.

Security controls – FileFlex acts as an additional control to manage access to unstructured data.

Consent Management – Access to unstructured data through FileFlex is through a consent-based approval process. Both owners and users must undergo a structured process to become authorized to access data. This process can only be accomplished through a consent based approach.

Data minimization – FileFlex enables organizations to limit the number of data duplicates required to conduct business activities while making it easier to manage where data resides within the organization.

Usage monitoring – FileFlex keeps detailed logging and audit information of all data access and authentication activities. Log information can then be consumed by enterprise Security Information and Event Management (SIEM) systems and security analytics platforms.

Breach Notification – FileFlex supports detailed auditing and integration with enterprise SIEM technologies. In turn, these capabilities enable faster response to security incidents and timely notification when incorporated as part of a comprehensive security program.