WHITE PAPER

GENERAL DATA PROTECTION REGULATION (GDPR) COMPLIANCE AND HOW EFT CAN HELP

GLOBALSCAPE

Failure to comply with the standard may result in significant fines for organizations based in the EU or with an EU presence.

May 25, 2018 is an important date for companies that provide a product or service to residents of the European Union (EU), as that is the day when the EU begins to enforce the General Data Protection Regulation (GDPR).

The European Commission established the GDPR to ensure that companies follow a set of security and privacy standards that help safeguard the fundamental rights and interests of "data subjects." The GDPR achieves this goal through the advancement and elaboration of seven overarching data protection principles, as documented in Article 5, sub-sections 1 and 2:

- Personal data is fairly, lawfully, and transparently processed.
- Personal data is secured against threats, destruction, loss, or damage.
- Personal data is kept accurate to the extent possible.
- Accountability in dealing with personal data must be demonstrated.
- The collection of personal data must be limited to explicit, specific, and legitimate purposes.
- The collection of personal data must be the minimal amount required to achieve its purpose.
- The collection of personal data must only be retained for the minimal period of time necessary to achieve its purpose.

Failure to comply with the standard may result in significant fines for organizations based in the EU or with an EU presence. This could also apply to companies based outside of the EU with no EU presence, depending on international treaties and the mechanisms for enforcement.

GDPR SCOPE

Globalscape has examined the scope of GDPR as it relates to on-premises software, self-managed in a public or private cloud, and cloud SaaS offerings, in addition to internal personal data processing and collection. The scope of GDPR can be broken into several categories, which are subsequently referenced throughout the GDPR readiness portion of this document.

GDPR's scope as it pertains to Globalscape's managed file transfer (MFT) software, EFT, whether it is deployed on-premises, self-managed in a public or private cloud, or in a SaaS-based capacity (EFT Arcus) is as follows:

- **Receiver:** EFT can receive files, which may contain personal data.
- **Storage:** EFT can optionally store files on a local or network attached disk upon receipt.
- **Sender:** EFT can further process received or stored files by transferring them to internal or external applications, systems, or servers, including to non-member states or organizations that may not adhere to GDPR standards.
- **Configuration:** EFT can optionally store certain personal data associated with authorized login accounts
- **Posture:** EFT can be deployed by customers on premises or in a SaaS configuration on computer systems or networks that may reside in the EU.

GDPR READINESS

Globalscape has assessed its data security and privacy strategy as it relates to achieving GDPR readiness within the aforementioned GDPR scope. But what is GDPR readiness mean? Is it the same as GDPR compliant? Unfortunately, there is no such thing as a GDPR compliant product, nor is there a single product that will make an organization compliant. GDPR readiness, when applied in context with software products, means that software applications that may fall within GDPR scope will provide an essential set of security, auditing, and governance controls to help achieve and maintain a "GDPR-ready" posture. When combined with other GDPR-ready products and the organization's GDPR driven policies, procedures, and controls, EFT can help facilitate compliance with the GDPR standard, at least as it relates to data passing through (receiving) or residing on (storage) or residing in (configuration), or transferred out of (transferring) their MFT ecosystem, wherever it resides (posture).

SECURITY, AUDITING, GOVERNANCE

Globalscape's managed file transfer product offerings, EFT and EFT Arcus, provide the following security, auditing, and governance features to help achieve and maintain a GDPR-ready posture:

SENDER AND RECEIVER

- Secure protocols to protect data in transit
- Full audit log to trace complete lifecycle of data
- Robust set of authentication controls over who can access data
- Mitigation against external threats provided by DMZ Gateway®
- Integration with DLP and data classification systems via the Internet Content Adaptation Protocol (ICAP) protocol. MFT solutions such as EFT deal mostly with unstructured files, rather than semi-structured data such as JSON or XML; therefore, the content of those files is almost completely opaque to the EFT platform. Because of this architecture, upstream or downstream processes need to exist to determine whether files that are processed through EFT contain personal data, including controls that would allow or disallow processing of said data. EFT's optional support for the ICAP protocol allows it to side-channel files that are being received or that are about to be processed, allowing a third-party system to examine and flag those files accordingly (disallowing further processing), or even modifying their content, including replacing personal or other sensitive data with alternate content.

RECEIVER

- Ad hoc, person-to-person (P2P) transfers protected through optional authentication layer
- Native mobile access client leverages Enterprise Mobility Management (EMM) and secure storage to mitigate external threats
- Optional multi-factor authentication further reduces risks from external threats

STORAGE

- Encryption options for protecting data at rest, including OpenPGP
- Optional secure data wiping, otherwise known as data sanitizing
- Local-managed or AD-managed access controls over what data can be accessed
- Automated, scheduled clean-up action helps comply with storage-retention requirements

CONFIGURATION

- User account information is always stored encrypted
- Removed user accounts are automatically purged from storage and memory
- Options for automatic removal of stale user accounts
- No personal data is every requested or collected from end users
- Personal data can be furnished by admins or by active directory. User account personal details (email, phone, full name, etc.) can only be furnished by an administrator or via an Active Directory server; therefore, it is up to the organization to implement upstream safeguards over how that personal data is obtained and whether it is obtained lawfully.

THE TABLE BELOW CAN SERVE AS A GUIDE IN REFERENCE TO HOW EFT CAN HELP ACHIEVE AND MAINTAIN A GDPR-READY POSTURE.

Any further questions about GDPR should be directed to your account rep, so that we can further assist you with your data management strategy. GDPR chapters and articles that are unrelated to product or organizational readiness, such as chapters that define the role and responsibility of supervisory authorities, have been excluded from this table.

GDPR ARTICLES	HOW ARTICLES ARE ADDRESSED WITH EFT
Articles 1-4 document general provisions. Article 5 outlines the principles related to processing of personal data. This article is in essence a high-level summary of what the GDPR means in reference to personal data. Those principles, as stated earlier in this document, include: • Lawfulness, fairness, and transparency • Purpose limitation • Data minimization • Accuracy • Storage limitation • Integrity and confidentiality • Accountability Articles 6-11 qualifies when collecting personal data is allowed, and the types of personal data and conditions that may apply, in addition to the need to obtain consent. EFT does not directly collect personal data. See Articles 12-14 for more on this.	EFT covers one or more of Article 5 principles in a number of ways: **Integrity and confidentiality** is achieved through encryption, auditing, authentication options including federated authentication, access-level controls, and non-repudiation receipting. **Accountability** is achieved via the segregation of administrator duties, as well as purpose-built reports that capture and report on product configuration as it relates to security standards, such the robust PCI DSS standard. **Accuracy** of user account personal data is either a manual process, modified directly by an administrator, or automatic, by nature of updates made to linked directory services, such as Active Directory or LDAP sources. Accuracy of file data is guaranteed via CRC and hash checksums. **Storage limitation** is covered by various controls in the product that limit the longevity of accounts and optionally the data (files) linked to those accounts. For example, stale users can be disabled or removed automatically from the system, or a specific date can be sent for account removal. Likewise, ad hoc, P2P file transfers can have expiring links, including one-time-use links, which limits the longevity of both the data, and/or the underlying user account. **Purpose limitation and data minimization** are largely upstream controls around personal data, if stored in files processed by EFT; however, EFT does provide controls to encrypt, wipe, and offload these files, through the construction of automated triggers and actions, such as “Every day, purge any file older than 30 days in the following directory.”
Articles 12-14 deal with transparency and rules around communication, with most of these rules affecting the processes and procedures related to the collection and processing of personal data.	EFT does not directly gather personal data from end users. Personal data can be gathered by external processes and then input by an administrator into EFT (see Configuration). Alternatively, data that is retrieved automatically via a directory services connection (AD, LDAP, etc.) would be subject to these requirements and require that the organization have a process in place to ensure that it obtained consent, disclosed reason for use, provides a communication process, etc.

GDPR ARTICLES	HOW ARTICLES ARE ADDRESSED WITH EFT
Article 15 deals with a person's right to confirm whether their personal data is being used, and whether the person has access to their data. Article 16 deals with rectifying inaccuracies in personal data. Article 20 deals with the right to receive their data in in a format that can easily communicated with others.	Qualified (authorized) administrators can determine whether personal data is associated with a particular user account, and can manually or programmatically export a user's account configuration data, including any and all fields that related to personal data, upon request. File data, which may contain personal data, is made available to end users via secure protocols and is subject to authentication and access controls, meaning authorized users can access their files directly, or a qualified administrator can access those files on the requesting user's behalf.
Articles 17-19 and 21 deal with a person's right to erase, restrict, or object to certain processing of personal data.	Although these mostly fall outside of the purview of EFT, EFT does provide the ability to disable accounts temporarily without removing them, as well as the ability to permanently remove them, including all associated details including files that might be considered personal data, and can optionally apply secure wiping of the user's files such that they cannot be reconstituted.
Article 25 espouses the concept of personal data protection by design and by default, rather than as an afterthought.	EFT was built with a layered approach to security and privacy, with the need to comply with PCI, HIPAA, and DoD requirements serving as primary drivers for Globalscape's "data protection by design" philosophy long before the creation of the GDPR standard. The security features and safeguards in EFT are simply too numerous to list in their entirety here, but are captured extensively throughout EFT's online documentation, such as the online help files.
Article 24 and 26 and 28-30 relates to the obligations of organizations depending on their role in processing or controlling data, and includes requirements on the need to record processing activities as part of the obligations of the processor.	EFT provides robust auditing of transactions as a receiver or sender, along with, configuration state changes, compliance readiness, and even administrator-documented compensating controls. Reports derived from this data help satisfy these requirements, as it pertains to data processed by EFT on behalf of the organization.
Article 32 is similar but less general that Article 25 offering specific advice, such as pseudonymisation and encryption of personal data, providing a means to restore lost or damaged data, maintain system resiliency and availability, amongst others. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller.	EFT provides both means for both pseudonymisation (specifically, use of aliases for usernames and contact emails), and encryption, ranging from built-in streaming encryption to OpenPGP key-based encryption. EFT provides a number of features to help maintain confidentiality, integrity, and availability, ranging from backup and restore to high-availability clusters, redundancy checking for file integrity, and roles, authentication, and access controls, along with extensive auditing to ensure confidentiality.

GDPR ARTICLES	HOW ARTICLES ARE ADDRESSED WITH EFT
Article 35 and 36 reference the need to perform a data protection impact assessment, especially when doing a large scale or automated or profile based processing.	Globalscape's professional services team can assist customers in their impact assessments in context with EFT in its handling of data. This assessment can include assistance setting up a Proof of Concept (POC), answering questions as to security and privacy capabilities, developing custom solutions, such as providing connecting users with DPO contact details, or providing you with a development platform on which you can assess any effects on operations before installing or upgrading EFT in our environment.
Article 37-39 deal with the situation where a data protection officer might be required, along with the role of the Data Protection Officer (DPO), which amongst other tasks, includes the need to monitor compliance with the regulation, ensure the proper assignment of responsibilities, and raise awareness and training of staff involved in processing operations, and related audits.	EFT provides a number of features that would aid a DPO or DPO-designated responsible party, including audit logs, audit tables, in-console monitoring of activity, and historical analytics, including diagnostics tables that track transfers end-to-end. EFT also allows for delegation and segregation of duties through the creation of subordinate "administrative roles," granting just enough access to those roles for them to perform their duties, which aligns with Article 5's data minimization clause.

FOR FURTHER INFORMATION ON GDPR,

or for more information on similar data security and privacy initiatives, including PCI DSS compliance, FIPS 140-2 compliance, and HIPAA compliance, please contact us here.

MAKE BUSINESS FLOW BRILLIANTLY

Globalscape, Inc. (NYSE MKT: GSB) is a pioneer in securing and automating the movement and integration of data seamlessly in, around and outside your business, between applications, people and places, in and out of the cloud. Whether you are a line-of-business stakeholder struggling to connect multiple cloud applications or an IT professional tasked with integrating partner data into homegrown or legacy systems, Globalscape provides cloud services that automate your work, secure your data and integrate your applications – while giving visibility to those who need it. Globalscape makes business flow brilliantly. For more information, visit **www.globalscape.com** or follow the blog and Twitter updates.

GlobalSCAPE, Inc. (GSB)
Corporate Headquarters
4500 Lockhill-Selma Rd, Suite 150
San Antonio, TX 78249, USA
Sales: 210-308-8267 / Toll Free: 800-290-5054
Technical Support: 210-366-3993
Web Support: www.globalscape.com/support

GLOBALSCAPE