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

GLOBALSCAPE
# CONTENTS

- INTRODUCTION ...................................................................................................................................................... 3
- GDPR SCOPE & POSTURE ............................................................................................................................................... 3
- GDPR READINESS .......................................................................................................................................................... 4
- EFT’S UNIQUE PRIVACY FEATURES .................................................................................................................................. 4
  - SUBJECT STATUS .......................................................................................................................................................... 4
  - PRIVACY POLICY & CONSENT ........................................................................................................................................... 4
  - EXERCISE RIGHTS ............................................................................................................................................................ 5
  - AUTOMATED TRIGGERS ......................................................................................................................................................... 5
  - LEAST ACCESS PRIVILEGE, ENCRYPTION, METADATA .................................................................................................. 5
  - DPIA REPORT ..................................................................................................................................................................... 6
  - AUDIT CONTROLS ............................................................................................................................................................... 7
- GDPR SETTINGS ................................................................................................................................................................. 7
- EFT’S STANDARD FEATURES ............................................................................................................................................. 8
- REFERENCES ......................................................................................................................................................................... 13
INTRODUCTION
On May 25, 2018, the European Commission began enforcing the General Data Protection Regulation (GDPR), affecting virtually anyone doing business within the EU or providing a service to residents in the European Union (EU), including organizations based out of the US or other countries, depending on applicable trade laws.

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

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

GDPR SCOPE & POSTURE
If your organization exchanges data with customers, clients, contractors, employees, or business partners, whether you use a dedicated Managed File Transfer (MFT) solution such as EFT, a set of REST APIs, or a hodgepodge of disparate services or scripts, there is a pretty good chance that either a subset of the data being transferred or the details associated with user accounts involved in the data transfer will fall within GDPR’s definition of “material scope.” In addition to territorial and material scope, the GDPR categorizes organizations as a data Controller or data Processor according to their posture.

As a Processor: Files or data originating from your organization that may contain personal data that is subsequently transferred to other organizations, including to organizations residing in non-member states, may be subject to Processor requirements.

As a Controller: Files or data originating from your business partners, employees, clients, contractors or any other data Processors, sent to your organization and subsequently stored on your network that contains data that the GDPR classifies as personal data (email address, IP address, phone number, etc.), may be subject to Controller requirements.

As both Controller and Processor: As data passes through or is stored within your organization, you may be subject to requirements as either Controller, or Processor, or both. For example, if you set up an account for a contractor so they can upload files to your organization, and you store the contractor’s personal email and phone number along with their account login details, then you are acting as a Controller. If those files are subsequently offloaded to a partner, and they happen to contain personal data, such as personal email addresses for a marketing list, then you are also acting as a Processor.
GDPR READINESS

Globalscape’s Managed File Transfer (MFT) solution, EFT, is the only MFT product on the market to provide a comprehensive set of privacy-related controls that facilitate GDPR readiness for organizations that are seeking to achieve GDPR compliance.

Keep in mind that there is no such thing as a GDPR-compliant product, nor is there a single product that will make an organization GDPR 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 and privacy 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 facilitate compliance with the GDPR standard, at least as it relates to file data passing through their MFT solution, or user account details required for business partner, employee, or client access.

EFT’S UNIQUE PRIVACY FEATURES

SUBJECT STATUS

- Flag user account owners as being EU data subjects
- Allow user accounts the ability to view their EU data subject status and to change their EU data subject status
- Audit changes to EU data subject including who made the change

PRIVACY POLICY & CONSENT

- Optionally display your organization’s privacy policy to connected users
- Specify whether consent with your privacy policy is mandatory or implied
- Capture and audit consent status changes for each user
- Allow users to rescind their consent
- Trigger a wide variety of automated tasks when consent is given or withdrawn
EXERCISE RIGHTS

- Allow partners or other users to exercise their GDPR rights
- Allow the right to access (view) any data flagged as Personal Data associated with an account
- Allow the right to rectify (modify) Personal Data directly by users
- Allow the right to object or restrict access to Personal Data, triggering a server-side event
- Allow the right to portability, where that user’s Personal Data is made available for download
- Allow the right to be forgotten, with a broad range of automated options

AUTOMATED TRIGGERS

- Create automated events when privacy rights are exercised by users
- Specify which conditions apply, and react depending on right exercised
- Choose from a large number of actions to react with, such as:
  - Delete the user’s Personal Data or restrict their Personal Data from modification
  - Terminate the user’s session and/or disable their account
  - Send a notification email to the designated Data Protection Officer

LEAST ACCESS PRIVILEGE, ENCRYPTION, METADATA

- New administrator-level permission for EFT administrator roles
- Personal Data permission controls to specify whether admins can view/modify a user’s Personal Data
- Any field considered Personal Data is masked for unauthorized admins
- Personal Data is stored encrypted at all times with a globally unique secret key
- Personal Data is decrypted on the fly when accessed by authorized users or administrators
- Authorized admins can specify which user account fields are considered Personal Data
- Authorized admins can also specify fields are visible, modifiable, or enabled
DPIA REPORT

• Run a DPIA report guaranteed from within EFT
• EFT considers all your privacy related settings and scores each one for risk
• EFT analyzes each user account and assess risk; for example:
  › Consent was rescinded but the account still has Personal Data associated with it
  › Account is flagged as being an EU data subject but Consent status is still unknown
• The DPIA report generates a Risk Score across a large number of GDPR Articles
• A relative risk score is computed, with a score closer to zero indicating less risk
• High risk areas are identified along with risk mitigation strategies
• Run the report from the admin console or via a REST API call
AUDIT CONTROLS
- Audit when authorized users exercise any of their rights
- Audit when authorized users grant or rescind consent to your privacy policy
- Audit when authorized users agree or disagree with your Terms of Service
- Audit when authorized users EU data subject status changes
- Audit before and after values for any field marked as Personal Data upon modify or rectify
- Audit when administrators change a user’s Personal Data and trigger an event to notify the user

GDPR SETTINGS
- Specify your Material and Territorial scope, which affects settings and reports
- Specify your Processing Principles, Lawfulness, and compliance with Age Restrictions
- Specify your Indirect or Direct methods for Collecting data
- Specify how Consent is obtained and can be rescinded
- Specify whether or not users are allowed to Exercise their Rights from within EFT
- Specify with Purpose, Necessity, Risk and Risk mitigation techniques for Personal Data collection
- Specify whether a Data Protection Officer has been assigned and supply their email address
- Specify whether Transfer Safeguards are in place, such as EFT’s Content Inspection feature
EFT’S STANDARD FEATURES

In addition to the set of industry-first and industry-unique set of privacy-related features, EFT provides a wealth of security features that are common to a broader set of MFT solutions. These features further enhance your organization’s ability to comply with privacy standards such as GDPR or security standards such as PCI DSS, especially as it pertains to file data that is moved through the solution on a transactional basis.

Sender and Receiver:
- Secure protocols to protect data in transit (FTPS, SFTP, HTTPS)
- Full audit log to trace complete lifecycle of data transfers
- Robust set of authentication controls over who can access data
- Mitigation against external threats provided by EFT’s secure proxy, DMZ Gateway®
- Integration with DLP and data classification systems via EFT’s Content Inspection feature
- Ad hoc, person-to-person (P2P) transfers protected via authentication or one-time passcodes
- Optional multi-factor authentication further reduces risks from external threats (CAC, SMS, SAML)

Storage:
- Multiple encryption options for protecting data at rest, including OpenPGP and Secure Folders
- 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

EFT ENTERPRISE PROVIDES ALL OF THESE FEATURES AND MORE, MANAGED IN ONE PLATFORM.
GDPR ARTICLE MAPPING

Any further questions about GDPR should be directed to your account rep, so that we can 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.

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

<table>
<thead>
<tr>
<th>GDPR ARTICLES</th>
<th>HOW ARTICLES ARE ADDRESSED WITH EFT</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Article 1</strong> document general provisions, while <strong>Article 2 and 3</strong> define material and territorial scope, which are critical in determining whether an organization must comply with GDPR. <strong>Article 4</strong> provides a glossary of terms and definitions of those terms.</td>
<td>EFT provides a configuration options for <strong>Article 2</strong> that lets administrators designate whether EFT falls within material scope, which captures whether the organization processes personal data, and whether those activities fall within Union law. For <strong>Article 3</strong>, EFT provides configuration options to specify territorial scope, including whether processing is occurring physically in the EU and thus EFT is in scope, or EFT is in scope due to international laws, or EFT is not in the EU but users might by data subjects. In the latter case, EFT provides further controls that allow admins to designate whether an individual user accounts is considered an EU data subject, including the ability for users to self-classify. These selections influence EFT’s posture with respect to GDPR and affect other privacy settings throughout the product, including the output and risk scoring captured in EFT’s DPIA report (see Article 35 below).</td>
</tr>
</tbody>
</table>
| **Article 5** outlines the principles related to processing of personal data. This article provides 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 | EFT covers **Article 5** principles in a number of ways:  
  **Lawfulness, fairness, and transparency**: EFT allows administrators to declare whether their deployed solution adheres to processing principals that, along with supporting documentation, affects the risk score computed in EFT’s DPIA report (see Article 35 below)  
  **Purpose limitation and data minimization**: EFT provides a number of controls to encrypt, wipe (secure delete), and offload files containing personal data to authorized systems via automated events.  
  **Accuracy**: For user accounts managed by EFT, personal data can be updated or rectified by administrators directly or via remote directory services, with controls in place to notify users in accordance with Article 19, or by users directly in accordance with Article 16.  
  **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 as the robust PCI DSS standard. |
<table>
<thead>
<tr>
<th>GDPR ARTICLES</th>
<th>HOW ARTICLES ARE ADDRESSED WITH EFT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Articles 6-8 pertain to lawfulness of process, the necessity of obtaining consent, and conditions applicable to minors.</td>
<td>Article 6 (Lawfulness of processing): EFT provides controls to set the basis for lawful processing, which are then captured into the DPIA report (see Article 35).</td>
</tr>
<tr>
<td>Articles 9-11 provide further qualifications around particular data categories and have no direct mapping to features.</td>
<td>Article 7 (Conditions for Consent): EFT lets admins configure whether end users can give and rescind consent, with specific actions tied to consent state changes.</td>
</tr>
<tr>
<td>Articles 12-14 deal with transparency and rules around communications, processes, and procedures related to the collection and processing of personal data.</td>
<td>Article 8 (Age Restrictions): EFT offers admins the ability to state whether age restrictions are applicable, adhered to by nature of EFT or external privacy policy or terms of service, or is affected by compensating controls. The choice is reflected in EFT’s DPIA report.</td>
</tr>
<tr>
<td>Article 15 deals with a person’s right to access any personal data helped by the controller.</td>
<td>EFT provides extensive configuration options around Article 15, including the ability to specify which user account fields qualify as personal data, and the ability to expose (or not) personal data fields to end users connected via the Web Transfer Client, in accordance with this article. File data transferred from/to EFT, 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.</td>
</tr>
<tr>
<td>Article 16 deals with rectifying inaccuracies in personal data, and is critical to achieving the “Accuracy” principle cited in Article 5.1(d).</td>
<td>If an EFT administrator elects to grant users access to their personal data (see Article 15 above), they will also be given the option to give users the ability to rectify or modify their personal data via EFT’s Web Transfer Client, in accordance with Article 16 rules.</td>
</tr>
<tr>
<td>Article 17, the right to erasure, better known as the right to be forgotten, pertains to a user’s right to have the data controller purge or expunge all records containing personal data, where applicable.</td>
<td>EFT provides a unique feature to help organizations comply with Article 17, where, if allowed by an administrator, an authorized end user can submit a request to be forgotten directly from within EFT’s Web Transfer Client. Administrators can configure EFT’s automation engine to react (or not) to a request to be forgotten, such as sending an email notification to the designated Data Protection Officer (DPO), deleting any personal data fields belonging to that user, immediately terminating their session, disabling or deleting their account, or any combination of these and more.</td>
</tr>
<tr>
<td>GDPR ARTICLES</td>
<td>HOW ARTICLES ARE ADDRESSED WITH EFT</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td><strong>Article 18</strong>, the right to restrict falls between the right to object (Article 21) and the right to erasure (Article 17). If, after objecting to use, it is determined that the organization failed to meet legal standards, but the subject is pursuing legal action, the user might pursue this right so their data remains unusable by the processor or controller pending the outcome of their claim.</td>
<td>Similar to Article 17 and 21, EFT admins can allow users the ability to exercise their right to restrict from within the Web Transfer Client in accordance with <strong>Article 18</strong>, and subsequently use EFT's event rules to automate any reaction to this right being exercised. This could be anything from a simple email to disabling the user’s account pending further investigation.</td>
</tr>
<tr>
<td><strong>Article 19</strong> covers the obligations of the controller to inform the data subject if their personal data has been modified or erased by someone or something other than the person themselves.</td>
<td>EFT provides industry-first controls to comply with <strong>Article 19</strong> by: 1. Auditing modifications to user account fields flagged as personal data, either by an authorized administrator, or by an external system (LDAP, AD, etc.) 2. Notifying the data subject if any external modification occurs within EFT under the conditions of Article 19. An event rule is triggered by the modification and sends the data subject an automatic email notification indicating that their personal data has been changed, along with before and after values.</td>
</tr>
<tr>
<td><strong>Article 20</strong> deals with the right for data subjects to receive their personal data in a format that can be easily communicated with others.</td>
<td>If authorized by an administrator, EFT allows end users to exercise their right to data portability according to <strong>Article 20</strong>, and obtain an immediate, downloadable copy of all their data flagged as personal data, in a semi-structured, human-readable file format.</td>
</tr>
<tr>
<td><strong>Article 21</strong> is the right to object, and typically is the first step in a process to the right to restrict (Article 18) or to the right to erasure (Article 17). Articles 22 and 23 pertain to automated decision making, profiling, and related restrictions.</td>
<td>Similar to Article 17 and 18, EFT admins can allow users the ability to exercise their right to object from within the Web Transfer Client in accordance with <strong>Article 21</strong>, and subsequently use EFT’s event rules to automate any reaction to this right being exercised. This could be anything from a simple email to disabling the user’s account pending further investigation.</td>
</tr>
<tr>
<td><strong>Article 24</strong>, and 26-31 relates to the obligations of organizations depending on their role in processing or controlling data. <strong>Article 25</strong> espouses the concept of personal data protection by design and by default, rather than as an afterthought and is applicable to EFT.</td>
<td>EFT was designed with a layered approach to security and privacy, driven by our customer’s need to comply with various security and privacy standards such as PCI DSS, HIPAA, and now GDPR. These means that for each new feature added to EFT, we follow a “data protection by design and by default” philosophy, in line with <strong>Article 25</strong>, documenting risk and devising risk mitigation procedures as part of the feature design, implementation, and test procedures.</td>
</tr>
<tr>
<td>GDPR ARTICLES</td>
<td>HOW ARTICLES ARE ADDRESSED WITH EFT</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td><strong>Article 32</strong> speaks to specific security tactics for protecting data, such as encryption of personal data, providing a means to restore lost or damaged data, maintain system resiliency and availability, among others.</td>
<td>EFT provides a unique, admin-configurable key that is only used for encrypting user account details flagged as personal data, as recommended by <strong>Article 32.1(a)</strong>. This means that even if EFT’s configuration database were compromised, the attacker would have access only to encrypted strings. EFT also addresses <strong>Article 32.4</strong>, with a new, industry-first feature consisting of a “right to view/modify personal data” permission that, if not set, will restrict the administration from viewing fields flagged as personal data, even when logged into the EFT admin console and independent of their other administrative privileges.</td>
</tr>
<tr>
<td><strong>Articles 33 and 34</strong> pertain to the organization’s responsibility to inform governing bodies and users of a breach. <strong>Article 35</strong> specifies the need to a systematic Data Protection Impact Assessment (DPIA) under certain conditions, to ascertain lawfulness, purpose, risk, risk mitigation techniques, necessity, and others.</td>
<td>In an industry first, EFT provides a built-in DPIA report generation tool that can serve as an input to your organization’s broader-scoped DPIA efforts in compliance with <strong>Article 35</strong>. Upon generating a report, EFT will evaluate the current state of its numerous privacy-related controls, audit any admin-provided rationale for Necessity and Proportionality (Article 35.7(b)) and Risk Mitigation Techniques (Article (35.7.d)), compute a risk score for all potential areas where privacy may be at risk, and output the report into a semi-structured format for either human consumption or for consumption via APIs or ingest into a reporting engine.</td>
</tr>
<tr>
<td><strong>Article 36–43</strong> cover a broad range of topics related to organizational responsibilities, from code of conduct to certification bodies. <strong>Article 37</strong> specifically outlines when a data protection officer might be required, along with the role of the Data Protection Officer (DPO).</td>
<td>EFT provides a configuration option to specify a designated DPO, in accordance with <strong>Article 37</strong>. The designated DPO can then be referenced via EFT’s event rule automation, such as in response to exercise of rights by users. Additionally, EFT audits all changes made by administrators with respect to privacy settings, request to exercise rights by users, and modifications to all data flagged as personal in nature. These are available to the DPO to review in either reports or directly.</td>
</tr>
<tr>
<td><strong>Articles 44–50</strong> references safeguards required when transferring personal data outside of the EU. The core functionality MFT solutions typically offers plenty in the way of securing data in transit and at rest. EFT’s primary differentiator is mentioned right.</td>
<td>EFT provides a number of features that can facilitate compliance with these Articles. One of those is the built-in Content Integrity Checker (CIC) feature, that, if enabled, instructs EFT to side-channel all files that are passed through it to a third-party DLP or similar data inspection device or application. Depending on the results, EFT can deny the transfer, trigger a notification, or perform other operations.</td>
</tr>
<tr>
<td><strong>Articles 51–99</strong> deal with remedies and penalties, methods for cooperating with supervisory authorities, and similar non-functional topics.</td>
<td>EFT has no direct functional mappings to the concepts covered the remaining chapters of GDPR; however, when EFT’s privacy settings are configured properly, it can facilitate GDPR-readiness so that the risk of penalties for non-compliance is significantly reduced.</td>
</tr>
</tbody>
</table>
FOR FURTHER INFORMATION ON GDPR, or for more information about similar data security and privacy initiatives, including PCI DSS compliance, FIPS 140-2 compliance, and HIPAA compliance, please contact us here.

REFERENCES
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.