Understanding and Implementing GDPR Compliance Measures

GFI Software™

October 2017

Contents

Introduction and Executive Summary

The General Data Protection Regulation (GDPR) was passed into law by the European Union Parliament in April 2016, with enforcement date beginning May 25, 2018. With the deadline quickly approaching, organizations are running out of time to determine whether and how the regulation applies to them and if so, how to implement changes in their IT processes that may be necessary to comply with the requirements.

The GDPR supersedes the Data Protection Directive (Directive 95/46/EC), which had been the basis of European privacy laws since 1995. Like most governmental regulations, the GDPR is a complex document and in some respects, is open to interpretation. The intent of the legislation is to protect the privacy of EU citizens and standardize the laws across all EU countries.

The good news is that organizations have many tools at their disposal to help them carry out and document the steps that must be taken to meet the GDPR requirements, from identifying the personal data that must be protected, to securing it properly, managing it effectively, and tracking its flow and where, when and by whom it is accessed.

Note: Whilst we are confident that the information contained in this whitepaper is accurate, it should only be used as guidance and not as legal advice.

GDPR Terminology

To understand the requirements imposed by the GDPR and how to comply with them, you first need to understand the meanings of some key terms and concepts that appear in the legislation. Unfortunately, the GDPR leaves some terms open to interpretation. For example, it requires organizations to provide a "reasonable" level of protection for personal data, but doesn't define "reasonable."

The following terms, along with others, are defined in Article 4 of the GDPR:

Personal Data

The GDPR's purpose is the protection of personal data, and unlike the previous Directive, it strictly defines the term instead of leaving it up to individual EU countries to do so. The GDPR's definition is very broad; it defines personal data as:

Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

This includes but isn't limited to basic identity data (name, address, phone number, ID numbers), biometric data, health and genetic data, web data (IP addresses, location, cookie information, and RFID tag data). Racial or ethnic data, sexual orientation, trade union membership, political opinions and religious beliefs are classified as special categories, or "sensitive personal data," and are subject to additional protections.

Data rendered completely anonymous so that individuals cannot be identified, directly or indirectly, is excluded from the scope of the GDPR.

Pseudonymisation

Pseudonymous data is different from anonymous data. Pseudonymisation may be a new word for many IT professionals; it means:

The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject ***without the use of additional information****, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.*

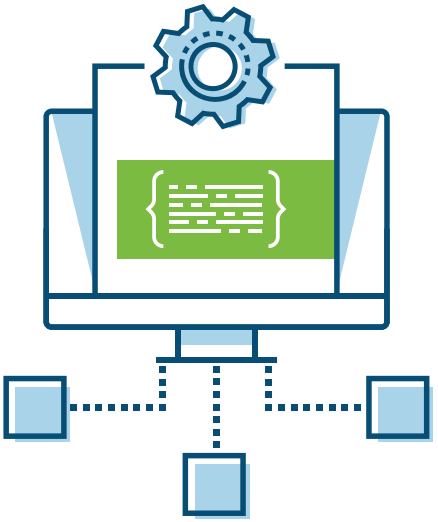
Pseudonymous data is still considered personal data, but may require lower levels of protection.

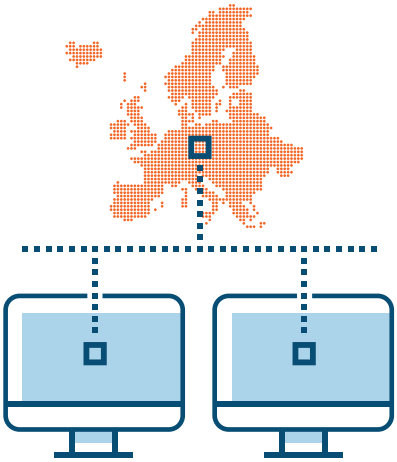
Processing

The GDPR imposes requirements on protection of data during processing, which it defines as:

Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means.

This covers a wide range that includes almost anything you can do with personal data: collect, record, organize, structure, store, adapt, alter, retrieve, consult, use, or disclose by transmission, dissemination or otherwise making available, as well as alignment or combination, restriction, erasure, or destruction of the data.





Controllers and Processors

The GDPR applies to organizations that collect, store, and/or process the personal data of European citizens. Both are responsible for compliance; however, the GDPR assigns different responsibilities depending on which of two roles the organization fills.

Under the GDPR, a person or an organization that alone or *jointly with others, determines the purposes and means of the processing of personal data* is called a controller. A person or an organization that *processes personal data on behalf of the controller* is called the processor. The same organization may function as controller for some data and processor for other data.

GDPR Overview

The first question every organization must answer in regard to the GDPR is "does it apply to us?" The GDPR increases the extra-territorial scope of applicability in comparison to the previous Directive.

If your organization is a controller or processor that is established in the EU, the answer is yes, even if the data isn't processed within the EU. However, even if your organization isn't established in the EU (that is, you have no physical presence there), if you offer goods or services within the EU or to EU citizens, or monitor the behavior of citizens in the EU, you are required to comply with the GDPR.

Other areas in which the laws have been tightened include:

- Mandatory breach notification within 72 hours of first becoming aware of the breach.
- The right of data subjects to request cessation of processing or dissemination of personal data, and to have it erased if the subject withdraws consent or if the data is no longer relevant (also known as the "right to be forgotten").
- The right of data subjects to be provided a copy of their personal data in a common electronic format upon request, and to transmit it to a different controller.
- Rules for obtaining consent from data subjects now require clear, plain language (no more hiding it within a sea of legalese) and withdrawal of consent must be easy.
- Privacy by design requirements that data protection be built into systems from the design stage.

A very important difference between the previous Data Protection Directive and the General Data Protection Regulation lies in the names: the former is a directive, while the latter is a regulation. A directive can be interpreted and implemented differently by different EU countries. A regulation is an enforceable law that is to be uniformly interpreted and applied across all of the EU.

For a full understanding of the GDPR, you must read both the articles (the law that was adopted and enacted) and the recitals, which set out the reasons for the provisions of an act and help interpret the meaning of the act. The GDPR consists of 99 articles and 173 recitals.

GDPR Impact

Because of the expansion of applicability mentioned above, many companies outside the EU that did not fall under the Data Protection Directive will have to comply with the GDPR. For example, "behavior monitoring" can include using cookies to profile EU citizens on websites.

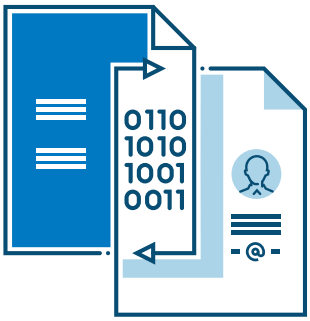
Many organizations will be forced to change the way they collect, store, process and protect customers' information. Companies who fall under the GDPR must assess their options and develop a compliance strategy. For example, you must decide whether to implement the same data protection measures for all personal data, or have separate data protection processes for EU citizens.

Some organizations will be required to appoint Data Protection Officers (DPOs). This applies to both controllers and processors when their core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale. It also applies to those who collect or process special categories of data or data relating to criminal convictions and offences. The DPO must be a qualified expert in data protection law and practices. The tasks of the DPO are laid out in Article 39.

The consequences of non-compliance with the GDPR can be severe; penalties vary depending on the nature of the infringement, but the maximum fine is the greater of 4% of annual global turnover or €20 million. To avoid this, U.S. companies are spending millions of dollars to meet the GDPR privacy regulations.

GDPR Requirements

Before IT professionals working for controllers and processors can implement solutions that will help the organization meet GDPR requirements, it's important to know what those requirements are. The GDPR requirements can be broken into a few broad categories, although these may also overlap.



Identifying and classifying personal data

The logical first step in protecting personal data is to identify it and distinguish it from other data that the company stores and processes. This means implementing a new **data classification strategy** or updating an existing one. Data classification involves finding and tagging personal data and sensitive personal data, and many organizations are already doing this as part of their overall security strategy.

Implementing a governance plan for personal data

Data governance refers to policies and procedures for managing and processing data, along with a plan for implementing those policies and procedures. The intent is to ensure that data is **uniformly managed throughout the organization**. In the words of the Data Governance Institute:

"*Data Governance is a system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which describe who can take what actions with what information, and when, under what circumstances, using what methods.*"

Your data governance plan is a fundamental aspect of meeting GDPR compliance requirements. To do so, it must clearly define roles and responsibilities for access, management, and use of personal data. Both processes and accountability are important elements in a data governance strategy.

Establishing procedures for personal data management

The GDPR imposes obligations on both controllers and processors related to how the personal data of EU citizens is to be managed. Controllers are required to:

- **Obtain consent prior to processing personal data (when consent is the basis for processing)**. Article 7 of the GDPR requires that consent must be given freely as a specific and unambiguous expression of the data subject's wishes. It cannot be inferred; the data subject must take clear, explicit action to opt in. Consent requirements for data that is classified as sensitive personal data, or that is the personal data of children, carries more stringent consent requirements, as specified in Articles 8 and 9.

- **Provide data subjects with specific information at the time the personal data is collected**. This includes details about the identity and contact information of the controller and its Data Protection Officer (if applicable), the purposes for which the personal data is being collected and processed, whether the data will be transferred to a country outside the EU ("third country"). The controller must also advise the data subject of his/her right to withdraw consent for the use of the data, and to request rectification (correction of errors or incomplete information) or erasure of the personal data. Data subjects must also be advised about transfer of personal data. Articles 15, 16, 17, 19, and 20 address these requirements.

- **Discontinue processing of personal data**. When a data subject withdraws consent, the GDPR requires that the controller discontinue processing, unless there is an alternate legal basis for processing it. Lawful basis for processing under Article 6(1) includes, in addition to consent, when processing is necessary for performance of a contract with the data subject, necessary for compliance with a legal obligation, necessary to protect the vital interests of the data subject or another person, necessary for performance of a task carried out in the public interest or in exercise of official authority, or necessary for purposes of legitimate interests pursued by the controller or third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. [**Note**: there are additional conditions for special categories of data].

- **Restrict processing of personal data upon request**. There are situations specified in Article 18 in which a data subject can request a temporary restriction on processing of personal data, but is still allowed to store it. Such situations include during a time when the accuracy of the data is being investigated, or if the processing is unlawful or the data subject has objected to the processing pending verification of grounds for processing. If the personal data has been transferred or disclosed to a third party, they should also be informed of the restriction of processing

- **Provide data subjects with a copy of their personal data upon request**. Under Article 20, under certain conditions controllers must provide the information in a "structured, commonly used and machine-readable format." The GDPR also requires that the personal data be transferred to another controller of the subject's choosing "without hindrance." This means you must demonstrate the ability to export such personal data in a common file format. This is known as data portability.

Protecting personal data through security measures

- **Take general and specific security measures to protect personal data**. The GDPR requires controllers and processors to implement "data protection by design and by default" using appropriate technical and organizational measures (Article 25). This can be demonstrated by an approved certification mechanism (Article 42). More specific security requirements include encryption and pseudonymisation. On a more general basis, Article 32 also requires that processors demonstrate the ability to ensure ongoing confidentiality, integrity, availability, and resilience of processing systems and services, and the ability to restore availability and access to personal data in a timely manner in case of a physical or technical incident.

- **Conduct testing, assessment and evaluation**. Processors must also show that they regularly test, assess and evaluate the effectiveness of their security measures, in accordance with Article 32.

Notification, Records maintenance, and reporting

- **Provide notification of personal data breach to a competent supervisory authority**. Article 33 specifies that controllers are required to report the breach within 72 hours of becoming aware of it. Article 55 defines a competent supervisory authority.
- **Maintain a record of processing activities**. Article 30 imposes the obligation on controllers and processors to maintain detailed records (audit trails) that demonstrate purposes and categories of processing carried out, categories of recipients to whom personal data have been or will be disclosed, any transfers to a third country or international organization, time limits for erasure of different categories of data, and description of technical and organizational security measures implemented. There is a limited exception for organizations employing fewer than 250 persons but it carries additional criteria and many organizations will not be able to claim it. Records must include tracking the flow of data to countries outside the EU or to third party service providers.
- **Carry out Data Protection Impact Assessments (DPIA)**. Processors are required under Article 35 to conduct a DPIA where processing uses new technologies and is likely to result in a high risk to the rights and freedoms of individuals. A DPIA is required in specific instances, including when there is large scale monitoring of a publicly accessible area; when evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based produce legal or other serious effects concerning the person; and when processing is conducted on the special categories of data referenced in Article 9 or 10 ("sensitive personal data and data related to criminal convictions and offense).

GDPR in the Cloud

The move to the cloud by many organizations means IT departments in many cases don't have as much control over the security of their data as they did when everything was processed on premises. In a cloud-centric enterprise environment where hybrid networks are commonplace, security is a responsibility that's shared between the cloud provider and its customers.

In such situations, to ensure your compliance with the GDPR, you need to know exactly where your responsibilities lie and what measures your cloud provider takes to secure the data you store and process through their services. Shared responsibility policies are published by Microsoft and Amazon for their Azure and AWS cloud services.

It is important to remember that even under a shared responsibility model, it is your organization that could ultimately be fined for not complying with the GDPR. Part of your responsibility is to choose the right cloud provider and to ensure that any optional security measures, such as two-factor authentication, encryption, and strong key management, are enabled on your account. You can't assume that putting your data in the cloud automatically guarantees that it is compliant.

Both Microsoft and Amazon provide information to customers regarding the measures they implement and what their services do to help you comply with the GDPR.

GDPR Solutions

When you have an understanding of the basics of GDPR terminology and impact, along with the requirements that need to be met in order to be in compliance with the regulation, you can develop an implementation plan. Your technical and organizational solutions will be aimed at accomplishing the specific requirements, and a multi-layered strategy will be needed to meet all of the requirements.

IT pros will be most concerned with the technological tools and security controls that can be used to identify, classify, manage, secure, track and document personal data that is subject to the GDPR rules. Luckily, there are many such solutions, whether you process personal data on-premises or in the cloud. In many cases, the solutions that you have already implemented as part of best security practices may be sufficient to meet specific GDPR requirements.

Some of the technological controls that will help you to comply with the GDPR are discussed in the following sections.

Data identification and classification tools

Solutions that help you to identify and tag personal data and sensitive personal data that are subject to GDPR mandates provide another critical component for your compliance implementation strategy. There are many third-party tools that can help with this, and the operating systems, database software, cloud storage services, and other solutions you already have in place include built-in mechanisms that can serve this purpose.

For example, you can use PowerShell scripts in Windows, Azure Search in Microsoft's cloud, query tools in SQL Server, and so forth to help you find data based on structure and pattern (such as social security numbers). Azure Information Protection (AIP), which is part of Microsoft's Enterprise Mobility + Security (EMS) solution, helps you classify data in Windows Server file servers, and you can create data classification rules for automatic file classification in Active Directory.

Amazon offers a service called Macie that automates the process of discovering, classifying and securing large amounts of data stored in the AWS cloud. The User Guide explains how to use Macie to classify data stored in AWS S3 buckets.

Data encryption solutions

Protecting personal data involves encrypting it both at rest (where it resides in storage) and in transit (as it travels on private networks and across the Internet). Encryption ensures that even if attackers are able to gain unauthorized access to your stored data or intercept data being transmitted, they won't be able to read it.

Encryption at rest solutions include full disk/volume encryption and file level encryption. Technologies such as Microsoft's BitLocker and Encryption File System (EFS), along with many third-party products, can encrypt entire disks or volumes. Managing encryption of portable devices can be especially difficult. You can use GFI EndPointSecurity to detect storage device encrypted with BitLocker To Go, configure different permissions, and encrypt the devices that are not secured. Strong encryption, such as 256-bit AES, should be used to encrypt personal data.

For encryption in transit, Transport Layer Security (TLS) is a standard protocol that provides strong authentication and protects both the confidentiality and integrity of data as it travels across networks. Personal data can be protected by sending it through the encrypted tunnel of a VPN connection. All web transactions that contain personal data should be protected by HTTPS. SMB 3.x with SMB Encryption enables you to encrypt data transferred over a network, including between virtual machines.

Major cloud services providers offer both automatic and optional encryption features that protect data in their storage services and in transit over their networks, and between clients and their data centers. Microsoft Azure services provide many encryption options, as does Amazon Web Services (AWS). Both support both client-side and server-side encryption.

Encryption is only as secure as the keys and secrets on which it depends. Encryption keys should be stored in a safe location and protected by a good key management system.

For encryption in transit, Transport Layer Security (TLS) is a standard protocol that provides strong authentication and protects both the confidentiality and integrity of data as it travels across networks. Personal data can be protected by sending it through the encrypted tunnel of a VPN connection. All web transactions that contain personal data should be protected by HTTPS. SMB 3.x with SMB Encryption enables you to encrypt data transferred over a network, including between virtual machines.

Major cloud services providers offer both automatic and optional encryption features that protect data in their storage services and in transit over their networks, and between clients and their data centers. Microsoft Azure services provide many encryption options, as does Amazon Web Services (AWS). Both support both client-side and server-side encryption.

Encryption is only as secure as the keys and secrets on which it depends. Encryption keys should be stored in a safe location and protected by a good key management system.

Identity and access management

Identity management is the foundation of data security. Controlling who has access to personal data is a necessary element in securing it to meet GDPR requirements, and so is management of customers' and employees' identities. A good IAM solution is essential to enable organizations to identify whose data they are storing or processing and where it is located, and can help manage consent and respond to data subjects' requests for rectification and erasure as well as imposing restrictions on who can access the personal data.

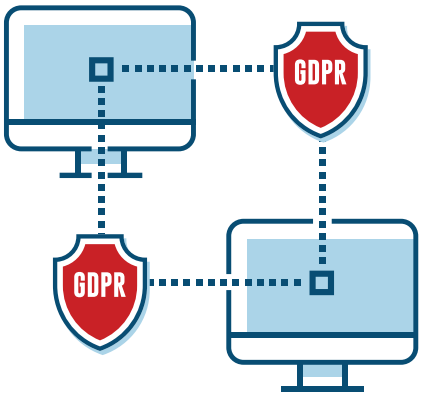
Windows Server Active Directory and Microsoft Identity Manager provide a simple IAM solution for on-premises data centers, but there are many third-party IAM solutions that can add features and functionality.

Identity as a Service (IDaaS) is a new approach to IAM being offered by a number of companies. Cloud providers have their own IAM solutions: Azure Active Directory (AAD), AWS IAM and Google Cloud IAM control access to the cloud services, and organizations with cloud and on-premises resources can use different IAM solutions in conjunction with one another.

For purposes of GDPR compliance, identity and access controls are used to restrict access to personal data, employing a principle of least privilege so that only those who need access will have it.

Network security and preventing data breach

Network security covers a wide range of technologies and is at the heart of any strategy designed to protect and secure personal data. This includes preventing unauthorized access through remote attacks and encompasses effective patch management, vulnerability assessment, firewalls, network isolation, multi-factor authentication for network logon, and more.



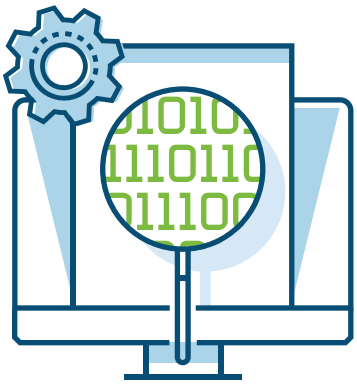
Solutions such as GFI LanGuard and GFI OneGuard can enhance an organization's ability to detect network vulnerabilities before they can be exploited and apply the appropriate security fixes to help protect against data breaches, as well as protecting against viruses in real time. Next-generation network firewalls and gateways with intrusion detection and prevention (IPS) capabilities, such as Kerio Control, help provide comprehensive network security measures that keep attackers away from the personal data on your network.

The web browser is a favorite attack vector for malware and data breaches, so it's important to ensure that web-based attacks don't result in exposure of personal data. There are many options for securing web activities and transactions, including proper configuration of browser settings. A solution that monitors web downloads for malicious software, such as GFI WebMonitor, can play an important role in protecting personal data.

Email security

Personal data is often transmitted via email, so protecting email communications is a vital part of GDPR compliance. Deploying an email security solution such as GFI MailEssentials can provide protection on several different levels: scanning for email viruses and malware, and at the same time enabling you to set and enforce content policies to prevent users from deliberately or inadvertently leaking personal data in violation of GDPR rules.

Security monitoring and incident response



Monitoring for indications of security breaches or incidents is a requirement of the GDPR, and there are numerous monitoring solutions on the market. The Windows Server operating system provides security event logs, but it can be difficult to find what you're looking for without a solution that helps you easily detect suspicious activities in real time so you can respond as quickly as possible. In the cloud, Microsoft's Azure Security Center can help you monitor for security events and set up alerts to detect threats.

While preventing or mitigating a data breach is the top priority, documentation is also crucial when it comes to compliance; you must not only be able to act – you must also be able to demonstrate later exactly when and how you took action.

An event management solution such as GFI EventsManager will give you more visibility into security-related policies, mechanisms, activities, and applications for faster incident response, and enables three-layer log data consolidation for compliance reporting that is protected by two-factor authentication. Such information can also be helpful in preparing a DPIA.

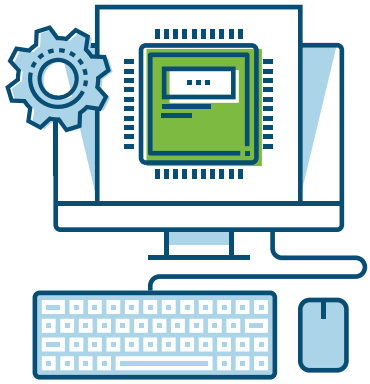
Audit trails and reporting

Network auditing is part of the testing, assessing and evaluating the effectiveness of your network security measures that is specifically mandated by the GDPR. Auditing tools are available within the operating system or cloud service, but this is another area in which a third party solution may enhance your ability to prove compliance.

GFI LanGuard, mentioned above, also provides centralized analysis and auditing of your network, which includes applications and configurations that can pose a security risk. It enables you to view the state of security applications, open ports, file shares, unnecessary services running on your computers, and a view of devices and applications on your network, all of which can impact the level of protection that is provided to the personal data on your network.

Hardware solutions

Deploying multiple solutions to address network access, viruses, malware, intrusion detection and prevention, VPN, and web content filtering can be expensive both up front and on an ongoing basis as it can quickly turn into massive administrative overhead. Small businesses on tight budgets, in particular, can benefit from an all-in-one unified threat management (UTM) device that serves as firewall, router, IPS, AV, anti-malware, VPN gateway and web and application filter.



The Kerio Control NG series of UTM devices provides protection that help to meet the security requirements of the GDPR and also produce reports that can be helpful in documenting GDPR compliance measures.

Centralized web based management with remote administration makes it easy to monitor and manage multiple Kerio Control deployments, and the devices interoperate with your existing environment, supporting Microsoft Active Directory and Apple Open Directory authentication as well as local user database authentication, and two-step verification for remote access provides stronger security.

Summary

Complying with the new data protection regulations that will go into effect in May 2018 under the GDPR is a huge and complicated task. However, for organizations that collect, control and process the personal data of EU citizens, compliance is not optional. Time is running out for companies to map out a plan for identifying, classifying, managing, securing, and documenting the protection of such data by implementing solutions that can accomplish each of the GDPR's requirements.

Using a combination of standard protocols and technologies along with features and functionalities built into your operating systems and included by the cloud provider in your cloud services, as well as third-party solutions such as those offered by GFI and Kerio, you can more easily implement measures that will help you meet the swiftly-approaching deadline for GDPR compliance.

USA, CANADA AND CENTRAL AND SOUTH AMERICA

Trilogy HQ, 401 Congress Ave #2650, 78701 Austin, Texas USA
Telephone: +1 (888) 243-4329
Fax: +1 (919) 379-3402
ussales@gfi.com

UK AND REPUBLIC OF IRELAND

Centurion House, London Road, Staines Upon Thames, Middlesex, TW18 4AX, UK
Telephone: +44 (0) 870 770 5370
Fax: +44 870 770 5377
sales@gfi.co.uk

EUROPE, MIDDLE EAST AND AFRICA

Mooslackengasse 17, Wien, 1190, Austria
Telephone: +43 (1) 928 7374
Fax: +43 (1) 25 3033 30035
sales@gfi.com

AUSTRALIA AND NEW ZEALAND

PO Box 375, Unley 5037, South Australia
Telephone: +61 8 8273 3000
Fax: +61 8 8273 3099
sales@gfi.com

For a full list of GFI offices/contact details worldwide, please visit http://www.gfi.com/contactus

GFI Software™