G.I.T.S.
Global IT Services PSF
Professionals of the financial sector (PFS)

General Data Protection Regulation

What can we do for you

GDPR

- HOW IS DATA COLLECTED AND STORED?
- WHY IS DATA BEING PROCESSED AND UNDER WHAT POLICY IS IT STORED?
- MONITOR AND CONTROL ACCESS TO PERSONAL DATA
- A RIGHT TO DATA PORTABILITY
- THE "RIGHT TO BE FORGOTTEN"
- THE RIGHT TO KNOW WHEN DATA HAS BEEN HACKED

For more information about our services or any of our solutions, contact: sales@gits.lu or visit: www.gits.lu

The GDPR transition is just around the corner but many organisations have yet to get to grips the full implications. The new GDPR regulation is mainly a legal story, regulations which need to be in place by May 25 2018. To assist with your preparations, this quick guide is to help you identify solutions that can help to be more compliant. In no case this can be considered as a complete GDPR solution. We will focus on some of the legislation's fundamentals and on IT-related security precautions GITS PSF can propose.

What is GDPR?

GDPR (General Data Protection Regulation) is a set of rules delivered by the European Commission, that enables people to have better control over their personal data. The key objective is that every person should be able to get a hold of its personal data such as names, addresses, telephone numbers, account details, online identifiers and other relevant personal information.

Who does this new law apply to?

In today's digital economy, personal data and privacy has acquired enormous significance. By unifying European rules on data protection, lawmakers aimed to create a consistent framework. Therefore, every European company or company that performs business in the E.U. and that stores any kind of personal information that makes it able to track and link to an individual, must comply to GDPR regulations.

How does GDPR affect your business?

1

The general guideline is that before storing information of individuals, you need to inform the individual that you will store, what you will store and for what purpose the person's personal data is needed and kept. Even more, no data may be kept on file if you have no reason to store that specific information.

2

Also, all stored information must stay up to date at all times. This implies that every change in address or phone number must be modified in the database immediately upon reception of the information. Individuals can also ask for data, if incorrect or incomplete, to be rectified whenever they want.

When you store data on a person, they have the right to demand a data transfer of all personal information towards another company. Also, when you are planning any cross-border data transfers, you have to make sure the transfer fits within the legal framework and the individual(s) have consented to the proposed transfer.

3

4

The rule about the right to be forgotten, can be quite challenging. When a person requests to eliminate all of the information that is stored about him/her, you are obligated to delete everything on that person from all of the company's storage carriers and lists. Including databases, backups etc. that are in place.

It is mandatory that a company has to report every data leak to the public. This implies that when your website, database or data storage is hacked and the hacker was able to access a database with email addresses or any other personal information, this leak must be reported within 72 hours.

5

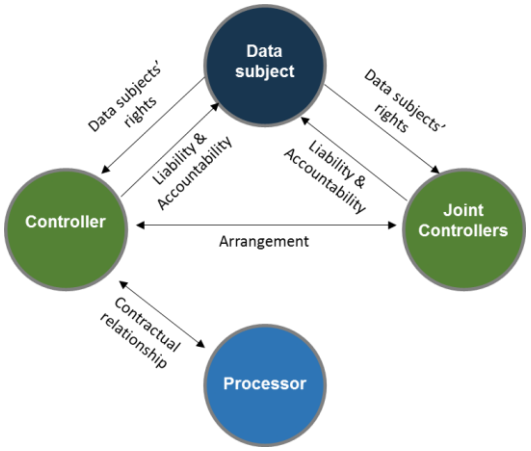
Data Protection Officer?

The need for a dedicated Data Protection Officer (DPO) applies for all EU and non-EU companies and is applicable to companies that sell goods and services or regularly monitor Europeans or process data on them at certain levels.

When data is your business and when you employ more than 250 people you are required to appoint and educate an official DPO or work with one on a contract basis.

GDPR data controller and processing framework

The law has emphasis on protection of Personal Data and rights of Data Subjects, including more transparency, explicit consent and access to data. Many principles under the GDPR are the same as the current Data Protection Directive 95/46/EC. Find below an interpretation of the framework:



Financial industry example

Data subject (natural person)
- Customers, employees, directors, third parties, delegates, etc.

Controller / Joint Controller
- Family Office
- Investment firm
- Fund administration
- Bank
- Application provider

Processor
- Primary IT systems operator of the financial sector

We encourage you to act on the GDPR regulation and as part of our obligation to our customers we believe that investing in protection and security of systems and data is something that all companies need to do, regardless of legal requirements such as GDPR. Below we present you an overview of the solutions in our portfolio that may help you to close some gaps and help you become more compliant for the new General Data Protection Regulation.

DATA LEAK PREVENTION

- **Proactive monitoring**
- **Controlled data processing**
- **Secure transfer via SSL encryption**
- **Anti-virus and malware scanning**
- **Two factor Authentication**
- **Disaster Recovery**
- **Strong password policy**

DATA PROTECTION

- **Next-Generation Firewalling**
- **Virus & Malware protection**
- **Intrusion Detection/Prevention Systems**
- **Deep Packet Inspection(DPI)**
- **URL Filtering**
- **Data protection policies**

END POINT PROTECTION

- **Anti-virus and malware**
- **Intrusion Detection firewalling**
- **Disk encryption**
- **Device control**
- **Removable Media Encryption**

For more information about our services or any of our solutions, contact: sales@gits.lu or visit: www.gits.lu

Solutions to ensure operational and business resilience

Downtime, a data breach or the loss of critical data can be disastrous to any business, reputation and brand. GITS PSF's solutions are designed to be compliant with European regulations.

Our team has many years of experience and specialized knowledge in guiding our customers towards compliant and regulated IT. We offer resilience and solutions aligned with EU data regulations and compliance standards for data protection. We ensure that your valuable data is processed accordingly and suitably protected.

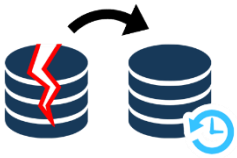
Data Protection by design

Abuse and interception of data is a serious threat that we take seriously to prevent. To reduce risks, we can implement state of the art measures such as multi-layer advanced firewalling, antivirus and malware protection, Intrusion Detection/Prevention Systems and Deep Packet Inspection(DPI) technologies to protect data, systems and networks.

Online backup and retention

The loss of business-critical data could have an enormous impact on a business. To prevent any loss of critical data we propose an enterprise-level (Online) Backup solution with a wide array of security features, backup policies, retention levels and compliance tools. The storage of data is done in separate secure containers with granular access rights, encryption in transit and at rest. We can guarantee the confidentiality of data.

Disaster Recovery and business continuity



We have tools to quickly recover data or services in the event of a disaster of critical business functions. Automatic fail-over of individual servers or complete environments, networks and security policies, while minimising downtime (RTO) and data-loss (RPO). We can design multi-site availability, for fast recovery times and optimised speedy recovery and restoration of data and applications in the event of almost any IT disaster.

Complete Endpoint protection

McAfee Complete Endpoint Protection helps to get security right. Offering one unified solution protecting PCs, Macs, Linux systems, servers and more. Reduce complexity, cut costs, and protect against rootkits, targeted web and email attacks, and persistent threats. You get powerful, efficient protection and encryption of systems and data with straightforward management and support by GITS PSF.

Data leak prevention and monitoring

Let us backup and secure your data. We monitor all services to avoid the possibility of data breach. One more step toward compliance by securing and hosting your data on our state of the art enterprise grade data storage platforms.

ONLINE BACKUP

- **Server and data backup**
- **Data Encryption at Rest**
- **Twin datacentre strategy**
- **Multi storage platform**
- **Secure containers**
- **Replication & deduplication**
- **Flexible backup policies**
- **Long term retention**
- **Flexible recovery options**

DISASTER RECOVERY

- **Automatically failover**
- **Multi-site availability of services**
- **Fast recovery time**
- **Decreased TCO through automation**
- **RPO and RTO**
- **Minimized data loss**

Sources

www.eugdpr.org

ec.europa.eu

www.pwc.com

www.deloitte.com

www.europe.eu

For more information about Business Continuity services or any of our other solutions, contact: sales@gits.lu or visit:

MANAGED HOSTING **BUSINESS CONTINUITY** **CONNECTIVITY** **MANAGED SERVICES**

G.I.T.S. Global IT Services PSF

Global IT Services PSF S.A.
12, Rue Guillaume Schneider
L-2522 Luxembourg
Grand-Duché de Luxembourg

Phone: +352 26 25 95 30
Email: sales@gits.lu
Info: info@gits.lu
Web: www.gits.lu