What the GDPR Means for You

What is the GDPR?

The GDPR (General Data Protection Regulation) is a regulation designed by the European Commission to create a uniform mandate for every EU/EEA member state on the protection of personal data held by an organization in the event of a data breach.

The current set of regulations found throughout the European Union (EU) and the European Economic Area (EEA) is derived from a directive that was commissioned in 1995 and was designed to be interpreted and formed within the national contexts of individual EU/EEA member states.

The new law is not a directive but a regulation that mandates all EU/EEA countries adhere to the same uniform law throughout the union, though some minimal level of variation may still exist within localized national contexts.

The GDPR is meant to align privacy laws throughout the European Union and protect the personal data of its residents at home and abroad. As a globally active organization, Therefore Corporation welcomes the new regulation as a step in the right direction towards strengthening personal privacy rights.

> "As a globally active organization, Therefore Corporation welcomes the new regulation as a step in the right direction towards strengthening personal privacy rights."

How Therefore™ can help:

The GDPR is a complex regulation that requires significant effort and investment in data security and protection by any affected entity.

Therefore Corporation strives to help you achieve compliance with the GDPR by offering an information management solution that allows you to store, find, and catalog the personal data retained by your organization and create a more secure data environment. Furthermore, Therefore™ offers resources that simplify the monitoring and management of the personal data you retain within the system, and provides tools to help you meet the GDPR's reporting and assessment requirements.

However, based on the broad scope and nature of the GDPR, it is important to recognize that GDPR compliance goes beyond software. Compliance is the result of a combination of sound data protection policies, procedures, training, and reporting. Therefore™ can help your organization achieve these results, and thus GDPR compliance, by providing tools which make it easier for you to discover, manage, secure, and report on the personal data your organization retains.

A correctly configured, maintained, and administered Therefore™ system helps you to securely handle personal information and provide more protection against data breaches when combined with proper organizational procedures, training, and operations.

How Therefore™ helps at a glance...

- Store, find, and catalog the personal data retained by your organization
- Simplify the monitoring and management of personal data
- Create a more secure data environment
- Tools to help meet reporting and assessment requirements

How do I get started?

The GDPR has many requirements about how your organization can collect, store, and use personal information. These include:

- How you identify, store, and secure the personal data in your systems
- How you accommodate requirements for data transparency
- How you detect and report personal data breaches
- How you train privacy personnel and employees
- And more

Since so much preparation is involved for adherence to this new regulation, Therefore Corporation recommends getting a head start on compliance preparations. Start reviewing your data management practices and policies as soon as possible. Non-compliance with the GDPR has the potential to cause serious financial or reputational harm to your organization; sanctions could include anything up to €10,000,000 or 2% of worldwide gross revenue, whichever is the highest. However, proof of a robust set of security provisions in place and the response time to reporting a data breach incident can be taken into consideration when the authorities are evaluating the situation.

You should start on the path to GDPR compliance by focusing on the following key areas:

DISCOVER: Prevention and Preparation

- Identify the type of personal data your organization collects and how you retain it
- Perform a risk assessment and threat analysis to get an idea of where you currently stand
- Appoint a Data Protection Officer (DPO)
- Train your staff to ensure data handlers are aware of the new regulation and how to adhere to it

MANAGE AND SECURE: Security Implications

Implement policies and tools to manage how the personal data you retain is managed and accessed:

- Prevent non-authorized personnel from accessing personal data
- Electronically: secure data in a way that is not openly accessible over the Internet or local networks
- Physically: prevent access to paper files, servers, or storage media where personal data is retained

Within Therefore™:

- Check your permission settings to ensure only authorized users have access to personal data
- Consider dedicating a high-security space in your Therefore™ repository, such as a folder of categories or a case definition, for the storage of personal data which falls under the scope of the GDPR
- Consider restricting View permissions on index fields which contain personal data
- Regularly review system access permissions by creating Security Reports in Therefore™
- Make sure you have enabled backup drives, storage and retention policies, and migration schedules to retain data properly
- Set retention policies to delete outdated information (after the retention period specified by applicable local laws)
- Enable advanced security settings in the Therefore™ Solution Designer if applicable and manageable
- For Therefore™ Web Access: consider enabling the "Encrypt Link" setting to mask objects IDs in Therefore™ for greater security

REPORT: Data Breaches and Actions to Take

Implement policies and procedures for dealing with and reporting data breaches:

- Maintain meticulous records of your organization's security implementations – robust evidence of efforts to protect and manage personal data increase the chances of leniency when it comes to sanctions by regulators
- Establish a procedure or strategy for effectively communicating a breach to your country's regulatory authorities – such breaches must normally be communicated within 72 hours

Within Therefore™:

- Configure Therefore™ Audit Trail to log actions taken by system users, and regularly review the logs for signs of suspicious activity.
- Store documentation related to your organization's security implementations in Therefore™, and build a workflow around the process of organizational review.

REVIEW: Privacy Policies and Subject Access Requests (SAR)

Implement policies and procedures for privacy policies ands SARs:

- Establish a protocol or procedure for handling subject access requests
- Regularly keep track of data protection regulations to ensure that business processes remain in-line with the law
- Update organizational privacy policies

Within Therefore™:

- Create a workflow for efficiently and correctly handling subject access requests and ensuring the process is fully documented and traceable
- Create a workflow to periodically remind you to check the latest regulations and adapt your policies and procedures
- Consider organizing personal data into logical groupings that make it easy to respond to SARs; for example, organizing customer files into cases, where all personal data related to an individual (documents, metadata, etc.) are grouped together
- Consider creating reports using Therefore™ Business Analytics to ensure processes are being completed appropriately
- Always install the latest recommended patches and updates to ensure your system remains secure

GDPR Implementation in Action

Let's look at a fictional case of an insurance company that uses Therefore™ to manage personal data in a GDPR-compliant manner:

Moya Insurance Group (MIG for short) is an international insurance company with headquarters in the EU.

Due to the nature of the insurance business, MIG retains a lot of personal data about its clients and is thus a prime target of the GDPR. This includes data such as:

- Name, DOB, marital status, home address, telephone numbers and email addresses
- Medical information and biometric data (for their health insurance sub-division)
- Income and financial information (for their mortgage insurance sub-division)
- Driving records and vehicle information (for their car insurance sub-division)

MIG uses Therefore™ to manage the data in their organization. They do so by organizing client files into cases, where all data pertaining to a client, including their personal details, documentation, and policy information is retained within an electronic version of a binder.

MIG understands the GDPR affects the way they do business. Here's how they've prepared to comply with the regulation:

DISCOVER

- MIG conducted a review of the records they retain and came up with a list of the types of personal data they retain about their clients

- MIG did not want to invest in hiring a new Data Protection Officer, so they contracted a lawyer for this purpose as needed
- The appointed DPO came to the MIG office and conducted a training seminar to educate MIG employees on the GDPR. Each attending employee signed off on their attendance. The training materials were saved in a Therefore category accessible to all employees for review at any time. The signed attendance sheet was saved in Therefore™ along with the other documentation MIG is creating while preparing for the GDPR

MANAGE AND SECURE

MIG conducted a first audit of their security policies with their IT department and found the following issues:

- A system administrator had quit 3 months ago and forgot to return his key for the server room. The lock was replaced for security purposes and the new key was distributed to authorized personnel.
- Filing cabinets in the basement with client information from 2005 to 2010 posed an additional risk. MIG decided to outsource the scanning and digitization of these paper documents, which they later imported into Therefore™.
- A hard drive with a copy of client documents was found on an employee's desk. MIG's policies were updated to forbid employees from taking client data off their network without prior authorization. MIG is now considering installing the Therefore™ Mobile App on their off-site employees' devices to enable secure remote access.

MIG conducted a review of their Therefore™ system and made the following changes to increase data security:

- In order to minimize the amount of personal data displayed, they changed their permission settings so managers could only view client data for their sub-division rather than the entire organization.
- They decreased the amount of time it takes for users to log out after a period of inactivity. This is to minimize risk in case an employee walks away from their workstation without locking it.

REPORT

- MIG created an additional category in Therefore™ for saving their documentation of security procedures, their implementation of protection measures, and evidence of their training activities around the GDPR.
- They also created a workflow that regularly sends checklists to department heads to review data handling protocols with their team members. The department head signs off on this review to continue the workflow.

- Together with their DPO, MIG established a protocol for reporting data breaches to the proper authorities within 72 hours. As part of their training, employees were also shown how to identify potential data breaches and how to report them.
- The Therefore™ system administrator at MIG configured Therefore™ Audit Trail to log when documents are exported or sent from the system. She then configured a workflow to remind her to review the logs on a weekly basis, save them in Therefore™ (along with the other compliance documentation) and report any suspicious activity to the DPO for further investigation.

REVIEW

- MIG established a workflow for handling subject access requests. This procedure is started when a client fills out a web form hosted on their website, which automatically starts a workflow in Therefore™. Since MIG organizes their client information in cases inside of Therefore™, it's easy for the employees handling SARs to find all pertinent information relating to a client.
- MIG has a regularly scheduled audit with their DPO to ensure the company's handling of their clients' personal data is still compliant with the GDPR.

Closing Remarks

All organizations that retain and process personal data are obliged to know that the GDPR will apply to them. Affected organizations are thus responsible for being informed about the regulation and complying with its provisions starting with the 25th of May 2018.

This document is for information purposes only and should not be considered a comprehensive guideline for legal adherence to the GDPR regulations. Affected organizations may need to seek independent legal advice while establishing or examining their processes for compliance with the legal requirements set out by the regulation, or any specific issues which may arise as a result thereof.

Neither the author of this document nor the organization he/she represents shall be held liable for the usage of this document in preparation towards adherence to the GDPR, or for damages resulting from non-adherence.