A certified response to GDPR

While businesses await the first GDPR decisions, certification already offers a route to compliance and will only become more important as the regulation beds in

BY JASON WALSH

Michael Brophy, chief executive of Certification Europe

The intended consequence of GDPR is the protection of user data. The unintended consequence, however, has been a panicked scramble for compliance, hardly a rational response to a regulation that has been well telegraphed.

"There's a sense of panic that this is all brand new, but that's not the case," said Michael Brophy, chief executive of Certification Europe.

As the May 25 deadline approaches, more and more companies have been preparing, many for quite some time, but the key, said Brophy, is preparedness rather than the illusion of being entirely compliant.

"The sort of companies we know, clients of ours, have been working on this for a year, some of them 18 months, but that's a small minority [and] even those who have been working on it for 18 months wouldn't say they're ready," he said.

"I think a lot of companies are more prepared than they give themselves credit for. The vast majority are already dealing with the data protection act. GDPR is building on that and of course it's bringing in new requirements, but no company is starting from a blank sheet."

One sheet many will be starting with is ISO 27001 certification.

ISO 27001, the international information security standard, prescribes best practice for information security management systems, and has an explicit role in the GDPR, said Brophy.

"That's the standard for an organisation if they want to keep any information secure. Personal information is a subset of information, it doesn't require a separate certification."

Brophy said that certification comes into play when it is time to test that systems, either designed in-house or built by consultants, are up to scratch.

"It's not just about ticking the box, it needs to be effective and efficient for your company. This will get you a long way down the road to GDPR compliance. Some of our clients estimate that ISO 27001 will get you somewhere from 75 to 80 per cent compliant," he said.

Looking at the detail of the GDPR, Brophy said that further certification will follow and that it is, in fact, a key aspect of the regulation's design for compliance. The aim, after all, is for widespread compliance, and not, as many have apocalyptically feared, tying up businesses in red tape.

In light of this, getting certified is certainly a clear route to compliance, and, crucially, to demonstrating goodwill.

"In the next 24 to 36 months there are [more] standards coming. This is the way it will go in the future. It's written in the GDPR itself: one of the mandates of the article 29 committee is that it is tasked with recommending standards [and also] under article 40 of the regulation it specifically says there will be recognised codes of conduct for certain sectors of industry."

Louise Kidd, head of liabilities and financial lines, AIG Ireland

Working from the top down to ensure data compliance

With GDPR fast approaching, larger organisations should make sure they have buy-in from all areas, especially from executive level, writes **Quinton O'Reilly**

With GDPR finally coming into effect soon, the onus is on businesses to ensure they have taken the necessary measures to be compliant.

While smaller organisations may find it challenging due to a lack of resources, larger organisations shouldn't assume they're safe because they have the budget and or resources.

GDPR requires every department to do their part, not just IT, and this is particularly the case for those in board of management or executive positions.

For compliance to work effectively, there needs to be a buy-in from the board along with every tier in the management structure of an organisation, said Louise Kidd, AIG Ireland's head of liabilities and financial lines.

"It's about understanding that there is now a need for long-term strategic planning around how a lot of existing processes within a business will need to change and adapt," she said. "Most companies are aware of the financial risks associated with data breaches, but it's also important they understand the cyber threats facing them.

"Expensive data breaches are now a fact of corporate life, and therefore it has never been more important that businesses consider a well-designed risk management framework to stay ahead of these various threats."

One major part of GDPR compliance is how management communicates to the business. Since this is something that has a significant impact on day-to-day operations, communicating the roles each employee must play, and providing the necessary training is crucial.

Chances are that most companies are aware of their current obligations, thanks to the existing data protection framework.

This acts as a benchmark to enhance the current framework they have in place to comply with GDPR.

"As part of this enhanced framework, it's important to implement prevention methods where cyber-resilience should be a primary focus," said Kidd.

"Virtually all companies have a business continuity plan (BCP) to deal with fire and flood events – all key stakeholders and management know what to do in an event of a serious incident like a fire by following its agreed BCP, but do they know what to do in the event of a serious cyber-attack?

> **Larger organisations shouldn't assume they're safe because they have the budget and or resources**

"A resilience plan is best developed by working across cross-functional groups like IT, marketing, and finance where roles and responsibilities are delegated to monitor threats both internally and externally."

All of this ties in with the key advice Kidd provides: be proactive. Most companies don't need to be reminded of the pitfalls associated with a reactive approach in any context, and the same logic applies to security.

"At AIG, we provide emphasis on our risk-mitigating solutions to stay ahead of these various threats," said Kidd. "These include providing our clients with pre-loss services and providing them with access to best in class legal, data, PR and IT professionals who have experience in dealing with live emergency cyber breaches.

"We also provide clients with knowledge, training & compliance solutions, IT security assessment services along with many others so they have a better understanding of their risk profile."

With that in mind, the best way to prepare for a data breach or cyber attack is to have a strong plan in place. Kidd said it is essential that companies have a disaster recovery plan in place, as well as adequate cover in case something goes wrong.

She also recommended that companies carry out simulations of a data breach and investigation, as it can show you how ready a company is and potential weak points which they can later refine.

"Carrying out a simulation is vital, so every employee knows the role they need to play and processes they need to follow," she said.

"Having a seamless breach plan in place should a breach occur is crucial, and it includes things like notifications to customers, putting a helpline in place, and an internal and external communication plan."

COMMERCIAL PROFILE: GLANTUS

Can you manage the right to be forgotten?

dt Transform
glantus

GDPR implies that organisations have to anonymise or delete personal data immediately upon request if it is no longer required for the original purpose stated.

GDPR is fast approaching

The new GDPR regulation prescribes that companies must be able to source, export and delete the personal information of any given individual across all their business operations on request.

This means that companies must keep an account of any personal information stored in their operational systems. Individuals now have a right to know if an organisation is processing their personal data and for what purpose. At any time, they can revoke consent for certain use of their data.

One of the main problems businesses are facing is inability to easily identify and access every piece of personal information connected to an individual, in order to ensure compliance and prevent prosecution.

The Solution

Transform GDPR, developed by Glantus, connects to all data held within operational systems, regardless of location, e.g. finance, HR, marketing, operations, etc. You can then simply classify all personal information within your systems to meet your GDPR requirements, easily linking data back to the individual. The personal information belonging to any given individual can then be tracked across as systems and departments.

Therefore all potential GDPR requests, such as the right to be forgotten, anonymise, etc. can be easily executed via the Transform application.

Transform GDPR can also be used for classification of other non-personal sensitive data, enabling users to closely monitor compliance on an ongoing basis.

Key features:

- Connects to any data source: Designed with usability in mind, with live connectors.
- One Click Classification: Identify, Tag and Group all your personal data via a simple user interface.
- Data Mapping: Link all personal data, across multiple systems with ease across all departments.
- Auto Retention Periods: Create and apply retention periods for specific data, automatically alerting the users for verification.
- Retains Data Integrity: Ensuring any update to your system is not going to break it.
- Who is it for? IT Managers, Data Officers...in fact anyone that needs to manage GDPR compliance

Watch our GDPR Video – visit www.glantus.com

About Glantus

Glantus is an innovative developer of business led data platforms and solutions.

For further information on Transform GDPR and other products, visit our website www.glantus.com, or call us on (01) 889 5300.

glantus

DATACONVERSION
Providing Data-Driven Software & Customer Experience Solutions.
+353 1 804 1298
dataconversion.ie

We help businesses improve performance in 3 key areas:

Customer Experience

Customer Engagement

Data Integrity & GDPR