THE EU GENERAL DATA PROTECTION REGULATION IS FINALIZED

WHAT'S IT ALL ABOUT?

The new General Data Protection Regulation is something that has been going on for several years. It will replace what was previously the European General Data Protection directive from 1995.

The idea was to build a consistent foundation across all European Union States so there's a basic commonality or consistency between what happens with data protection and critical infrastructure. This has been going on for several years now with the European Commission to establish what that regulation is with several drafts from 2012. The final draft was formally agreed in December 2015. That draft finally went to the European Parliament on April 14th this year and has since passed. The General Data Protection Regulation will now take effect twenty days after it's been passed in Parliament, which means on May 4th, the clock for the two years' transition period starts.

The regulation is focused on ensuring any nation state, organization, or company dealing with European citizens' personal identifiable information are obliged to comply with this regulation. It is really to ensure that organizations dealing with personal data of European citizens have a certain standard that they have to comply with. This means data protection, adequate security measures are in place, privacy by design when there is a breach, or disclosure of information. They are obliged to notify the national authority of the country where they operate within 72 hours of the breach. After they have an obligation to – depending on the risk value of the information that's been compromised, if low risk or high risk, – notify the impacted party without undue delay.

Now there is a foundation of taking responsibility and accountability when it comes to dealing with European citizens' data.

As a result of the accountability and responsibility, it means that excessive collection of information is now accountable because the more information you gather, the more accountable, and responsible you become. Now in case there is a breach and it is found that adequate security measures were not in place, there are significant penalties and fines in place—20 million euros or 4% of annual turnover.

Previously, companies that would have decided that since there is no penalty or accountability, in case there is a breach, there is no business justification to really do adequate security. They would deal with it when it happened. Now they have the penalties and fines to look at and whether they are willing to compromise security or security now becomes a priority.

Organizations who collect or process European citizen's data- What are the consequences?

Depending on the type of relation that you have with European companies – whether you have companies which are subsidiaries of companies based in Europe or are providing services to European customers directly – the regulation will apply to those businesses.

For those companies that have operations in Europe and have subsidiaries or either a supply chain outside of the European Economic Area, those companies that deal with European citizens, European data, over the two years' period will be transitioning to this new regulation. This means, of course, they have to comply with the regulation. They will have to look at the risks through their subsidiaries and also through the supply chain to see if, when they are moving their data to international locations, that puts them at risk of non-compliance with the regulation.

As this transition period starts and the companies within the European Union now have to comply with the regulation, the global companies will have to adjust as well. They will look to pass on the regulation potentially through what's called binding agreements or regulations that allow countries to have equal legislation.

For companies, which do not have subsidiaries or offices in the European Union, but are based in other international locations and/or provide services to European citizens directly, like online banking, online shopping, online retail, they need to have a Data Protection Officer who'll be based in the EU to ensure that these companies comply with the regulations.

This now means that the following principles will apply as a result of this major milestone:

- Adequate, relevant and not excessive
- Need to know principle / Least privilege principle
- Fairly and lawfully processed
- Obtained only for specified purposes
- Accurate and up-to-date
- Processed in line with the rights afforded to individuals
- Not kept for longer than necessary
- Not transferred to countries outside the EEA without adequate protection
- Accountability
- Kept Secure

At this time alternative methods are now being researched due to the recent ECOJ declared Safe Harbor invalid in October 2015 and the new EU-US Privacy shield framework has now been established with the foundation of the EU General Data Protection Regulation is setting a high bar.

This regulation is now driving companies to take out Cyber Insurance to reduce the risk against such penalties or fines.

- **83% have already allocated budget with 21% allocating $0.5 million or more to address the changes**
- **Top concerns include new penalties (42%) and tighter consent requirements (37%)**

Industries Impacted by the NIS Directive

Security and notification requirements for operators of essential services are concerned operators of the following sectors:

- Energy: electricity, oil and gas
- Transport: air, rail, water, and road
- Banking: credit institutions
- Finanial market infrastructure: trading venues, central counterparties
- Health: healthcare providers
- Water: drinking water supply and distribution
- Digital infrastructure" internet exchange points, domain name system service providers, top level domain name registries
- Digital service providers: online marketplaces, cloud computing services, search engines

Have to take appropriate security measures and to notify serious accidents to the relevant national authority.