The webinar is dedicated to the General Data Protection Regulation (GDPR) two years after implementation: Where do we stand? - What consequences on businesses, but also on the functions of risk manager and internal auditors and where are we going?

This webinar is a follow up to the one organized last year to discuss the results of a joint (ECIIA Ferma) survey.

As a reminder, the GDPR entered into force in May 2018. It establishes the first solid floor for comprehensive privacy protection in the EU. The new regulation created, therefore, a single set of data protection rules all across Europe!

In the European Risk Manager report of this year, cyber threats continue to be the most significant threat to the organisation's growth prospects within the next 12 months. We can clearly see today, with the increase of remote working, that cyber vulnerability increases and data management and use is expanding.

ECIIA has just released the Risk in focus 2021 edition, the survey has been conducted by 10 members and Cybersecurity and Data Security have been rated as top risks by 79% of the participants. The second risk is about regulatory changes and compliance. And the third one is about digitalization technology and artificial intelligence.

1. **Evaluation report about GDPR, two years after implementation-Mr Micol, Head of Data Protection Unit, DG Justice, European Commission**

- The Data Protection Unit of the Commission oversees the implementation of the GDPR in Europe. There is another department dealing with the International Data Flow covering issues such as Brexit and the EU-US Privacy Shield.
- **Some years ago, it was very difficult to raise the attention of the board of a company to data protection, and now it's very rare that this topic is not on the board's agenda**. This

issue is now brought to the higher level of organisations. It has created a kind of wake up call, maybe because there are financial penalties.

- **One of the main conclusions of the evaluation report is that that the Regulation does not need to be amended. Work must be done as regards the implementation and the enforcement.**
- The GDPR has become in a few years' time one of the few EU legislations that citizens know, even its acronym, which is very rare for a legislation made in in Brussels.
  Almost 70% of EU citizens are aware of the GDPR. And very importantly, we have the same proportion of people who are well aware that they have a national authority they can contact, which is their National Data Protection Authority (NDPA).
- The data protection authorities have different powers: they advise companies, make recommendation but also sanction… and they are fully independent; the EC is monitoring this independence.
  The 27 NDPAs have to create a common European data protection culture and harmonize the way they think and behave.
- A **lot of companies have used the GDPR as a way to distinguish themselves from the competition and to support their innovation.**
  The tracing applications developed for Covid 19 are in line with the GDPR, they have showed the importance of data protection.
- So, where do we need to improve? **The work of the data protection authorities is key**: they need the necessary resources, both human, and technical, given the expansion of data management and use with the development of artificial intelligence, data bases, blockchain, …
  We also need more uniformity in the implementation by all the member states. There are some areas where we have different rules (eg age of consent for children).

- **GDPR is considered as a steppingstone. It means that the approach followed with the GDPR will serve as a model to support the building of our European data economy.**

- We have the recent judgement of the Court of Justice on the data flows to the US. The EC is drawing lessons from these judgements, working on standard contractual clauses for transfers.

Poll question 1: how would you assess the level of divergence in the enforcement of GDPR regulation by the Data Protection Authorities in Europe? Is it high, medium, or low?

Results

GDPR has taken away a lot of the divergencies but still, the interpretation of how it should be implemented, can be improved: for example, for data breaches notification, there are different approaches between member states

Poll question 2: How do you evaluate your interaction with the Data Protection Authority in your country? Is it very good, good, bad, or very bad?

Results

For 72%, it's good.

For 20%, it's bad, and for 6%, is very good, and very bad for one person.

It is re-assuring. It shows the default of some data protection authorities in reaching out to stakeholders while others have good interaction with their stakeholders. The Commission is pushing the data protection authorities to engage more with stakeholders, especially when they develop guidelines, for instance, to have more feedback from the industry.

2. Lessons learned after 2 years of GDPR implementation, Jerome Avot, Chief Risk Officer and Data Protection Officer, Faurecia

The implementation of GDPR is positive for us:

- we made a full inventory of all the applications and the data processing activities we have and acted on those which were not (fully) compliant.
- Data security has improved: access, retention of data, and when we are starting a new application or a new product, we define the retention policy from the very beginning now.

- Since there is areputational risk, the release of budget for security related projects has been facilitated.
- it has changed the mindsets, including the relations with subcontractors incuding requirements for certification and also audits.
- most companies are now ready in case of a Data Breach. They know how to deal with new data processing (i.e. privacy by design) and are used to respond to Data Subject Request.
- wider training programs for employees regarding data protection (MOOC, massive online open courses) have been developed and have contributed to the reinforcement of the overall cyber security of the company.

Today, we are more efficient because we know where the data are located, and we're also working a lot in self-service mode. For instance, the employees know exactly which kind of data we have about them because they have access to those data directly.

We created a more security-oriented mindset, so that employees know that when they are exchanging Excel file with some personal data inside, they have to be very careful.

Jerome is DPO and Risk Manager and it seems a good combination to him: for instance, one of the tool of the GDPR is the Privacy Impact Assessment, which is a risk analysis. As a DPO, you need to have some bit of legal knowledge and some information system security knowledge as well. But you also need to be a pedagogue, to communicate and train people. You need a strong internal network and finally, you need to be able to assess risks.

And assessing risks is key, because it is based on this assessment that you will be able to design the actions to be taken.

Being Risk Manager and DPO has many benefits:

- Benefits from "risk oriented" mindset and ensure perfect alignment with Risk Management methodology
- Good mix between daily actions as a "DPO" and more medium/long term action as "Risk Manager"
- Being able to assess this specific risk at the right level in the overall risk matrix

The main ongoing challenges to deal with the current context are:

- **It is important to ensure continuous GDPR compliance: ensuring that all new and existing data processing activities are recorded and compliant; ensuring that all changes are being done in compliance with the GDPR regulation.**
- **The second one is about spotting the "weakest link", which could lead to a data breach Sometime the weakest link is just the sub-contractor laptops that could be stolen.**

The invalidation of the Privacy Shield is an issue and clear guidance must be released asap.

The Covid-19 outbreak poses a real challenge. We need to ensure the health and safety of the employees, while ensuring the compliance with the GDPR requirements. We see that the health related information is classified as "a special category of personal data" under the GDPR, meaning that a Data Protection Impact Assessment should be done in order to understand the risks associated with such kind of data processing and to ensure that those risks are properly mitigated. It means that we must identify clear needs, identify the "legal basis for processing the data", prepare a "privacy policy" and ensure security.. And finally, we must make sure that all those questions are being fully documented,

It has been a bit complicated at first because all people in Europe were asking themselves what they should do, but we received a lot of help from the Data Protection.

3. Lessons learned after 2 years of GDPR implementation, Ralf Herold, Senior Vice President Corporate Audit BASF

- The general experience with GDPR has been positive. But it is important to understand that it is not just about the protection of data but also the freedom to do business and the flow of information in the EU.

- It goes further from a business point of view.
  To protect the rights of the individuals, companies must take into consideration different dimensions: the nation/Government regulatory frameworks(Data Privacy Shield,..); the company contracts (IP Rights, antitrust regulations,…), The data subjects in the enterprise (employee contracts, customers contracts, vendors contracts,…).Companies must adhere to all of these and any change has a big impact.
  In Germany, GDPR has been initially about protecting the individual against the government
- Before GDPR, the data protection officer function was combined with the head of corporate audit (until May 2018). **As internal audit needs to audit the function of the data privacy protection officer, we moved the DPO from a company point of view/country point of view to a European level; we have mirrored the way the authorities working together.**
  The DPO is responsible to deal in Europe, we do not have any rule by company or by country, just for Europe and de facto global rules. With this, we can minimize the discussions and the interpretations and manage fast, have one opinion, unspecific for each topic.
  Internal audit needs to audit data protection, data privacy, as legal compliance. They do this in the design, implementation, and effectiveness, as part of the usual plan.
- New technologies come and go, artificial intelligence, blockchains,….and some authorities want to close markets. It is important to understand that whatever happens in the future, including technology, will depend on how the legal framework, the governments agree to deal with each other. **In Europe, having the same common market approach and the same conditions predictable, is a great advantage.**
- **Data protection privacy will work if it is embedded in the day-to-day operations**.
- It is also important to understand that products are developed in the US, Japan and China, even India, they come in the European market, so that's why they need to be compliant as well. **So we recommend a very short and simple approach: to use the GDPR as a starting point, as a template, and to rollout the "Spirit" everywhere in the world.**

CONCLUSION

Business is about trust and data privacy protection by design generates trust towards all business partners.

It can be a competitive advantage, if applied, effectively, which means it must work in practical terms.

The European Commission is in close contact with the DPAs to ensure that there are improvements made so that GDPR becomes a competitive advantage for all European companies. The stability in terms of GDPR regulation will also help the business.

Avenue des Arts 41
1040 Brussels, Belgium
TR: 84917001473652
info@eciia.eu
ECIIA

Avenue de Tervueren 273
1150 Brussels, Belgium
TR
enquiries@ferma.eu
ferma