Cyber-Security Council GDPR session

Yugo Neumorni

John McCarthy

Abstract

The majority of European companies are already in process to become compliant with the new GDPR regulation but very few of them are compliant.

The CIOs and IT business function are involved in GDPR compliance process but they do not lead the process. The processes is led by Risk, Compliance, Legal or other departments but CIOs have a huge responsibility in this process mainly in IT security area.

IT budgets are increased due to GDPR and the DPOs could support the increased IT budgets

There is a general understanding that this process does not end at May 25th. Some voices said that it actually begin in May 25th

Abstract

GDPR exists since many years but they were not applied consistently across Europe. Some countries in the West like Germany or UK seems to have a better experience in applying current / existing data protection legislation while others from Central and Eastern Europe were not very accurate in applying the law.

While the GDPR is a EU directive in some countries there was not implemented into the country's legislation yet (ex: Romania)

GDPR seems to be applied slightly different across Europe. This cause lots of confusions when multinational companies try to apply common procedures across the business units spread geographically in multiple countries/continents.

Huge interest regarding Right to be forgotten on backups or legacy systems or unstructured data.

Confusions regarding Data Controllers and Data Processors regarding the GDPR compliance

DPO outsourcing

- Outsourcing of the **DPO function**, how and who should own the responsibility ultimately within the organization?

Right to be forgotten. Backups

- There is still confusion about the need to remove data from cold backups upon request by the person who’s data is stored. There needs to be a uniform way of treating this across Europe.

  Is there ay real clarity and consensus on how the archives should be handled with regard to the required response to "requests to be forgotten", is it okay for the deletion to take place only when an archive is recovered

Data controller - Data processor. Cloud

- The contracts that are in place for the use of Public Cloud offerings tend to be very generic and inflexible, is it considered an obligation of those suppliers that they will align themselves with GDPR as well as their subcontractors.

Data controller - Data processor.
Cloud

- In the case of purchasing a cloud service that may use Personal Data within the processing, we have a responsibility as a controller, do the other parties involved have to declare their compliance to GDPR as suppliers or as processors? In this case they are just supplying the platform or application on which the data is processed.

- Currently an analysis of the Dutch DPA stated that Windows 10 and Office 365 are not considered GDPR compliant. MS will probably provide an answer in the near future, but has not yet been able to demonstrate compliance. What is the expected reaction of industry on this? It is impossible to cease using Windows 10 or Office 365. What is industry supposed to tell the employees who's personal data are considered at risk? What is the government telling the general public who's personal data is at risk?

Windows 10 and Office 365 non-compliance

Certification and code of conduct

- **Certification and code of conduct** are referred to in the regulation to support GDPR compliance. Can you give an update on the certification and code of conduct. What is in the pipeline? Who is working on these topics? When will they become available?

- How much is GDPR and "compliance by design" a driver for new Architecture principles? Impact of GDPR on complex IS landscape to implement certain requirements as “Data subject consent” by Processes, technical solutions, up to amendment of employee contract).

Compliance by design

GDPR Monitoring

- Continuous monitoring of GDPR Compliance after May 25th, how to get organized? Should we use the same external auditors as our current Financial ones? Any best practice there?

Right to be forgotten

- The "**Right to be forgotten**" may not apply to all circumstances, especially those where data is being processed under the lawful basis for processing being either "Contract" or "Legitimate Interest" does the team think this to be the case (for example Pension payments)

Different / contrary / conflict of interest regulation on EU Country?

- The laws on retention of data differ from country to country, even from sector to sector within a country. There may even be conflicts of interest between privacy regulations saying you need to destroy personal data as soon as it is no longer relevant, while other laws may require you to keep certain data for historical purposes for instance or to be able te reconstruct certain trains of thought etc. Where keeping track of legal requirements within one country may already be difficult for organizations (including DPA's), across Europe this will be virtually impossible. Some sort of central repository of such requirements should be set up, to be used both by businesses/organizations that operate in several countries as well as bij DPA's that are the 'leading DPA' for a multinational organization

Data breach notification different across EU?

- **Data breach notification:** can an overall approach be used in all over Europe? At this moment, there are different approaches by DPA, from allowing a simple phone call to filling out an extensive PDF document. It seems strange that this effort is copied for each DPA, and deviates for each DPA. A central European notification portal, preferably with the opportunity to set up an interface, would be both beneficial for international organizations and the cost of setting up and maintaining the solution.

Data breach notification

- **Data breach notification**: how will the DPA react on a notification?
  What is the purpose of the data breach processing at the DPA?

DPIA Different approach across EU

- **Data protection impact assessment**: can an overall approach be used over Europe? CNIL proposed a tool to support a DPIA, which seems to get adopted, judging from the different languages that are included. Other DPA are preparing or distribution guidance and/ or tools. The effort is multiplied, and the result is a disperse set of approaches, making it difficult for both industry and inspection purposes. A European approach would benefit international organizations and reduce cost of ownership

Right of access

- **Right of access**. The Data Subject has the right of access. Depending on different opinions, this access has to be within a time frame of 1 or 2 months or 4 weeks. It would be helpful to have practical guidance on how to react this an other kind of requests in common situations: request of an employee during or after employment, request of a registered customer with access to a portal, ...

Data controller - Data processor

- In real world situations, it is not always easy to define controller, processor, joint controller. The Swift case is an illustration of defining controller/processor, but also typical situation as the bank executing the payroll payments on behalf of the employer, a company, hiring the support of a facility management supplier, who hires people via an Interim company, ... Additional guidance would make the discussion with suppliers easier. This scenario's, though very common, result in discussions without clear consistent answers.

- What tooling is used to manage the personal data registration, if this is certified and if there are certifications for processors that comply with GDPR (which would make it easier for data controllers to know if their suppliers are an asset or liability with regard to GDPR compliance). Would be nice to discuss that.

Data controller - Data processor. Personal data registration tools

- How to master the impact of the massive shift to cloud (liabilities, negotiations with Cloud hosting providers)?

Cloud

- With employee data that is used for payroll, etc, is there a recommendation on the time it should be held and if so. is this consistent across member states. If there is no consistency, then is it recommended that data is held in organizations that cover many countries for the maximum period.

Employee data retention. Different regulation in EU

- • How far have attending companies come when it comes to data deletion? Will they be ready by 25.05.?
  • What is overall feeling of attending companies in that meeting how far they have come overall with GDPR?
  • Are there any best practices which can be shared amongst participating companies?
  (e.g. IT controls which helps to secure data)

Data deletion. Compliance

- What will trigger a potential GDPR audit from local Data Privacy authorities? Only based on a user request/complaint, or can they be random?

GDPR audit compliance

- The question is which are the best practices or the trends in approaching Article 32 as stated below.
  “Technical and Organizational Measures related to Article 32 (Security of processing): “Pseudonymisation and Encryption”: Status of art for Structured and Unstructured Data protection
  • Applicative Vs Architectural approach
  • Experiences in adopting encryption at Enterprise Bus level

Article 32 (Security of processing)

- How to leverage GDPR as an opportunity to increase data management & governance at company level (eg data model, master data management, data lineage)?

Data management

- How will be the relationship between the GDPR and ePrivacy directive look like ??

  Commissioner Gabriel recalled the problems of implementation of the current ePrivacy Directive which does not consider new communication services offered over the internet. She explained that the ePrivacy Regulation is needed to ensure a harmonised approach and avoid fragmentation.

GDPR and ePrivacy

GDPR and ePrivacy

- *A broad majority of businesses insisted on the need to fully align the ePrivacy Regulation with the GDPR (including the need for the risk based approach of the GDPR), challenged the Commission approach that metadata are sensitive per se and would like to ensure flexibility when entering into negotiations with the Council. Some businesses pleaded for "quality over speed". Few stakeholders asked to remove machine to machine communication from the scope of the Regulation. Businesses also raised the issue of settings rendering browsers as gatekeepers. A stakeholder asked to introduce exceptions for software companies to access metadata.*

  VP Ansip explained the differences between ePrivacy and the GDPR and mentioned the issue of sensitive data. He underlined that the Commission adopted a balanced proposal but also expressed openness to discuss with stakeholders on metadata and cookies. He insisted on the importance to find the balance between protecting privacy and innovation. Industry needs to be cooperative in order to find the right balance. Finally VP Ansip proposed to hold the next roundtable after the Council has defined its position on ePrivacy Regulation – around June.

Did you outsource the DPO function? What do you feel about DPO outsourcing?

Who’s leading the GDPR process in your organization? Risk management; HR; IT; Legal?

How do you find the GDPR compliance of the suppliers / customers / outsourced services imposed to Data processors by Data Controllers?

Did the GDPR decrease your cloud adoption appetite or IT outsourcing services considering the obligation of GDPR compliance of suppliers?

Can the authorities use GDPR abusive to destabilize the economic environment?

Additional questions

Could GDPR be used against non-EURO companies?

Do you expect an increase of IT/Security/Cyber budgets?

Do you expect a decrease of cybersecurity attacks in the future?

Do you think that cybercriminals might use GDPR as a new motivation?

Could the GDPR stop/minimize the personal profiling process on search engines (Google) or Social networks (Facebook, LinkedIn)?

Additional questions