05

Complying with Data Privacy Regulations (such as GDPR), up to full Board awareness

Yugo Neumorni
CIO Council Romania

Thierry Auger
Lagardère

What we found !

The key conclusions from the session

- We all have the same issue and concern, the subject is complex
- How we measure that our company is compliant: we have some steps, we are able to report were we are step by step but we need to continue to manage the process (evolutions, improvements, new needs...)
- We can close the gap by using technologies, but it is also necessary to deliver awareness and deploy training and to have the support of the board. Society should be educated for GDPR and cyber

What we have explored

Among these conclusions, we have developed one of these in greater detail below

A/ Governance / organization
- A governance supported by the board is mandatory
- The data governance must include necessary rules CSO can manage efficiently the mission
- Only a task force involving, the GDPR, the compliance, IT, the legal, impacted business
- A strong program manager rather than a DPO
- Where the DPO must be attached?
- The DPO as a service, could be an adapted solution
- The DPO a position for the future
- IT charter or the IT security policy must describe what is forbidden for final users

B/ Contracts
- Difficult to manage when we have a lot of contracts
- How can we ensure that providers are able to put in place necessary adjustments?
- We need clauses validated at European level, this must be done
- We must be able to cover an end to end compliance

C/ Legal information published
- A need, the big issue is on the consent, a strict opt-in process will kill the business, it's different from one country to another, we have to find the right balance, difficult for sale organizations.
  - Is-it a strict opt_in? No, just sometime when necessary

D/ PIA (Privacy impact assessment)
- For new projects, we need a privacy by design solution
- For legacy, we mainly use a questionnaire able to detect if a specific PIA must be done.

E/ Register of treatments
- We need a tool, not only to register treatment but also to discover what we have!

F/ Suppression, anonymization, pseudonymization, Purge
- Difficult on legacy systems
- Important to be able to demonstrate that you have done all that was possible

G/ Security adjustments
- We need to be able to detect easily our assets
- We need to follow the shadowIT
- Hard drive must be encrypted
- External support must be encrypted
- Encryption solutions must be deployed
- We must be care about some systems or applications unable to protect correctly our data
- Reinforce access management
- We must have answers to cover different needs we have to address (Privacy by design)
- Management of unstructured data
- We need a policy, final user must sign a responsibility document
- Data classification is an important process

H/ Data monitoring on networks and management of markers
- By using specific tools and markers

I/ Incident management
- A process must be put in place

J/ Awareness
- Just mandatory

K/ Budget
- Many budgets impacted: Legal, IT, HR for awareness & Training, compliance...
- Small and medium businesses might not cope with the GDPR compliance budget

What we have left open...
Some questions still remain to be addressed

where the DPO must be attached?

We agree that all of you search the best tool to encrypt (by delivering transparency for final users)
Right to be forgotten in cold backups almost impossible

Convergences
What points do we share in common

- Many things were not managed these last years, GDPR cannot be the only reason to launch them now
- For an international perimeter, Policy must be generic to cover globally all cases, local specificities must be managed with local authorities and regulation
- And all topics above

Differences
What points do we agree to disagree

/

A picture is worth a thousand words
An illustration that sums up our results