Roundtable with Business Associations on Privacy Shield, GDPR and ePrivacy
20th September 2018

Input European CIO Association

EU-USA relations

1. Legal status Privacy Shield needs to be confirmed

Where Privacy Shield aims at making trans-Atlantic transfer of personal data possible under a level of security that matches the level in Europe, many of our members are still weary to use it. As long as it's not clear if the Privacy Shield will hold up in Court, this instrument poses a risk to doing business and may lead to extra costs in renegotiating agreements to include model contract clauses later on if Privacy Shield is found to be insufficient. This situation needs to be cleared up. Does the Commission have any news on this topic and on the governance relating to the position of Ombudsperson?

2. Different approaches between EU and USA on data protection and security

There seems to be differences of approach between the US (nationality based) and EU (territory based) regulations relating to personal data protection and access to data for governments. Especially the contradictions between the US CLOUD Act in relation to GDPR impose great difficulties. What steps are or could be taken to repair the divergence in approaches and contradictory regulations on both sides of the Atlantic Ocean?

GDPR Implementation

3. Companies are struggling with the practical implementation of the GDPR, as guidelines are still coming, and the experience is growing.
EuroCIO believes there is a serious opportunity to help companies, small and large by providing extra pragmatic tools and guidance, to prevent all companies need to reinvent the wheel. Some examples:

- **The "Right to be forgotten" on Cold Backups.**

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

  Is there any 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? EuroCIO pleads for an approved workaround, as it is technically impossible to erase a person from a cold backup.

- **Different / contrary / conflict of interest regulation in EU Countries**

  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 to 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. We hear even DPA's are struggling with this.

Could the European Commission set up a central repository of such requirements, to be used both by businesses/organizations that operate in several countries as well as the DPA's?

- *A generic template to check the GDPR compliance of suppliers*
  Companies have tens or hundreds of suppliers. Especially for providers of cloud, payroll,…. Services companies are sending out their questionnaires or contract proposals to check the compliance of the GDPR. There is really an uncontrolled growth, although the same kind of questions pop up, but differently formulated, or in a different order.

  These are only a few examples. EuroCIO is happy to provide more examples.

ePrivacy Regulation

4. Don't redo GDPR

Many of our members will be impacted, although not as much as with GDPR. Impact on e-commerce, marketing and mobile networks will have largest impact on business. Indications are that the costs for implementing this regulation on top of GDPR is becoming disproportionate, especially as many of the data subjects seem to have no problems with leaving their data with service providers across the world.
Furthermore, where businesses are asking the European institutions and governments to harmonize and clarify the legal situation regarding to personal data protection, the European Commission seems to introduce even more legal uncertainty with the ePrivacy regulation.
We strongly urge to leave all personal data protection to be governed by GDPR only, and to focus the Regulation on Privacy and Electronic Communications on the confidentiality and other aspects that are not already covered by GDPR.