What about compliance (with GDPR)?

Prof. Lilian Mitrou
Dpt of Information and Communication Systems Engineering
University of the Aegean
The Institute for Privacy Law, Data Protection and Technology (IPL) – EPLO

Regulatory Technology and Compliance

- Regulatory Technology – "the use of technological solutions to facilitate compliance with, and monitoring of regulatory requirements" (Colaert, 2017)./
- Compliance with the law
- Emphasis on monitoring, reporting, compliance
- Focus on digitization of (manual) reporting and compliance processes
- To reduce human errors / restrict liability
- To quickly identify non-compliance :to prevent, respond to and remedy risk
- To improve (non) compliance visibility
- To modernize compliance

Emergence of RegTech

- Regulators efforts to enhance the efficiency of supervisory tools
- Enhanced compliance requirements
  - GDPR – emphasis on these aims
- (High) Cost of (non) compliance : Fines and civil liability
  - To reduce risk to organization
- Developments in data science and Artificial Intelligence
  - Enhanced data integration, use of automation, predictive analytics and strategic process alignment that may facilitate (strong) data governance and mapping regulatory compliance provisions

Accountability and Compliance

- A data controller must be able to demonstrate their compliance with data processing principles and with the regulation)GDPR Article 5 par. 2 / Recital 74)
- “to act in a responsible manner, to implement appropriate actions, to explain and justify actions, provide assurance and confidence to internal and external stakeholders that the organisation is doing the right thing and to remedy failures to act properly” (Felici, 2013).
- Accountability instruments like appropriate data protection policies, data protection by design and by default, IT security risk management, data breach notifications, data protection impact assessments, prior consultations and Data Protection Officers.
- Appropriate and effective internal processes and tools to implement these policies.

RegTech and Data Protection Officer

- Monitoring, analysing and reporting the GDPR compliance status in an organisation is the task of the DPO
  - Consultancy, Guidance, Record of Activities / Data breaches/ DPIA
- RegTech should not (be conceived and designed/deployed so to) replace the DPO
- It could "assist" the DPO by enhancing her ability to track organisational compliance progress, identify areas of compliance weakness and benchmark their performance against other organisations

RefTech Main tools for

- Data Governance and Data Discovery
- Consent Management/ Accountability: tracking and demonstrating consent
- Data Mapping – Relation to Register of Activities
- Data Breach Incident Response Solutions

In combination with tools/ instruments as

- Data Protection and Security Policies
- Awareness/ Education
- Certification of compliance insrruments and mechanisms

Compliance monitoring instead of compliance?

- (Personal) Data processing and protection interacts with the rest of the organisational activities/structure and the respective data management.
- Compliance monitoring presupposes compliance
- EDPS – Accountability Tool: I am not trying to sell you just another box-ticking exercise or some sort of quasi-automatic excel sheet. That would not only increase eadministrative burden, but also the risk of failure to truly embed accountability in the organisation. There is no such thing as culture change by check-list! (G.Buttarelli, Former EDPS)

References

- Article 29 Data Protection Working Party 2010 Opinion 3/2010 on the principle of accountability
- *Giovanni Buttarelli , The accountability principle in the new GDPR*
- Paul Ryana, Martin Craneb and Rob Brennanc , Design Challenges for GDPR RegTech
- IAPP 2019 The GDPR Maturity Framework <https://iapp.org/resources/article/the-gdpr-maturity-framework/>

Thank you for your attention

Prof. Lilian MITROU
L.mitrou@aegean.gr