TOGAF® Poster Series #67

GDPR and Enterprise Architecture – A Quick Primer

Good e-Learning

I would imagine that most practicing Enterprise Architects have at some point in the last six months been asked a question about the new General Data Protection Regulation, or GDPR, at the very least.

Awareness of the content and implications of this EU regulation, which comes into force in May 2018, varies wildly. Many organizations are playing catch-up. What most people understand by now, though, is that the costs of non-compliance are going to be very serious.

Here I'm going to briefly offer a few points that Good e-Learning feel every Enterprise Architect should know.

EXPANDED TERRITORIAL REACH

Due to its expanded territorial reach, the regulation will catch organizations that process or monitor the data of EU subjects, even if the organization is located outside of the Union. As Article 3 states, the GDPR will apply to " ... the processing of personal data of data subjects who are in the [European] Union by a controller or processor not established in the Union". This is not currently the case, and many organizations may have to appoint EU representatives. And yes, the GDPR remains relevant to the UK post-Brexit.

AN OBLIGATION TO DEMONSTRATE COMPLIANCE

The GDPR introduces many new accountability obligations placed upon organizations to demonstrate compliance (Article 5). With requirements such as maintaining certain documentation, conducting data protection impact assessments, and implementing data protection by design (e.g. data minimization) Enterprise Architects are in an ideal place to help. Modelers can provide transparency and analysis of data security across processes, people, and systems.

OTHER NEW DIRECT OBLIGATIONS

With the implementation of the GDPR, data processors will have direct obligations for the first time. Included in these is the obligation to record all processing activities. Furthermore, organizations will be duty-bound to record what is done with personal data and for which purpose (Article 30). Enterprise Architects with successful models may find that they are already half-way down this road, and could find themselves indispensable.

AN OBLIGATION TO DEMONSTRATE COMPLIANCE

Attempts to obfuscate over a breach will no longer be feasible under the GDPR. Data Controllers must notify data breaches within 72 hours of initial awareness, both to the authorities and to the data subjects concerned.

OTHER NEW DIRECT OBLIGATIONS

Fines for non-compliance under the GDPR are tiered in approach, enabling the imposition of "... fines up to 20,000,000 euros, or in the case of an undertaking , up to 4% of the total worldwide annual turnover" (Article 83). As you can see, for some organizations this would present a threat to ongoing operations. Personal damages may also be pursued by data subjects, with the personal liability of senior staff.

AN OBLIGATION TO DEMONSTRATE COMPLIANCE

Enterprise Architecture was born out of the desire to reduce financial, operational and reputational risk. It has evolved to play its part in ensuring regulatory compliance, and by definition offers transparent views of organization and process. Enterprise Architects will undoubtedly be in key positions to facilitate GDPR compliance within their organizations. And given the specter of large penalties, reputational risk and personal liability that will be stalking the c-suite, their place at the table will be open. Good e-Learning are planning online GDPR training, including certification and awareness courses.There will be live events and publications.