DEFeND Architecture: a Privacy by Design Platform for GDPR Compliance

Abstract. The advent of the European General Data Protection Regulation (GDPR) imposes organizations to cope with radical changes concerning user data protection paradigms. GDPR, by promoting a Privacy by Design approach, obliges organizations to drastically change their methods regarding user data acquisition, management, processing, as well as data breaches monitoring, notification and preparation of prevention plans. This enforces data subjects (e.g., citizens, customers) rights by enabling them to have more information regarding usage of their data, and to take decisions (e.g., revoking usage permissions). Moreover, organizations are required to trace precisely their activities on user data, enabling authorities to monitor and sanction more easily. Indeed, since GDPR has been introduced, authorities have heavily sanctioned companies found as not GDPR compliant. GDPR is difficult to apply also for its length, complexity, covering many aspects, and not providing details concerning technical and organizational security measures to apply. This calls for tools and methods able to support organizations in achieving GDPR compliance. From the industry and the literature, there are many tools and prototypes fulfilling specific/isolated GDPR aspects, however there is not a comprehensive platform able to support organizations in being compliant regarding all GDPR requirements. In this paper, we propose the design of an architecture for such a platform, able to reuse and integrate peculiarities of those heterogeneous tools, and to support organizations in achieving GDPR compliance. We describe the architecture, designed within the DEFeND EU project, and discuss challenges and preliminary benefits in applying it to the healthcare and energy domains.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 787068