ENSURING COMPLIANCE TO GENERAL DATA PROTECTION REGULATION (GDPR) USING E-SAFE COMPLIANCE

Author: Ahmad Jawwad

Published: October 2017

1 INTRODUCTION

General Data Protection Regulation (GDPR) imposes a new set of security requirements to protect personal data. These requirements are based on the experiences of data protection authorities and the everyday digital environment where cyber-criminals trade personal data in underground data markets. Any **data controller** (organization that collects data from EU residents) [1] or **processor** (organisation that processes data on behalf of the data controller e.g. cloud service provider) [1] must apply security measures and safeguards that allow it to implement the necessary standards for the protection of that data.

The solutions used, or safeguards applied, for protecting personal information can be:

i) Organisational (e.g., training of staff dealing with personal data, insist on non-disclosure agreements, put in place BYOD policy, appointment of data protection officer (DPO) etc.)[2,3,4],

ii) Physical (e.g., on premises security, disposal of any sensitive print outs etc.)[3] and,

iii) Technical (e.g. classification, discovery, continuous monitoring and auditing, protection, and identification of breach etc.)[1,3]

2 E-SAFE COMPLIANCE – BYOD, CLASSIFICATION, DISCOVERY, CONTINUOUS COMPLIANCE AND AUDITING, PSEUDONYMISATION AND NOTIFICATION

e-Safe Compliance fulfils the requirements of implementing a BYOD policy, classification and discovery of **personal data**, continuous compliance and auditing, protection of **personal data**, placing access controls to it and the identification of any breach of such data under the organisational and technical safeguards requirements of **GDPR**.

2.1 BYOD

e-Safe Compliance supports working from home scenarios and is BYOD compliant. In the case of a user, working as a **data controller or processor,** using their own machine, the system differentiates between the user's data and the controller's or the processor's data. Meanwhile, continuous compliance, auditing and protection mechanisms remain active for the controller's or the processor's data at the user's machine.

2.2 CLASSIFICATION, DISCOVERY, CONTINUOUS COMPLIANCE AND AUDITING

The module of Data Centric Audit and Protection (DCAP), enables organisations to fulfil the regulatory and legal requirements of classification, discovery, continuous compliance and of auditing the usage of personal data for GDPR. e-Safe Compliance's Information Classification Tool allows them to directly specify personal data and so offers an efficient means of performing data classification. In order to identify and classify personal data, following methods are provided in e-Safe Compliance:

1- Sensitive words and phrases such as EMR, electronic medical record, VIP, Title etc.
2- Standard and administrator defined regular expressions such as credit card numbers, Account numbers, Identification numbers, email address, computer IP address etc.
3- Definition of file names such as staff*.doc, staff-incent*.xls etc.

In addition to that, e-Safe Compliance offers a scanning utility, which is based on the rules, and scans local, network and shared drives to discover and locate personal data and information. The utility allows information owners or admin to define the location of the shared folders containing personal data, and to set the scanning frequency. Once defined any new file created in this location is automatically scanned based on the rules defined and gets monitored.

Furthermore, the information security management workflow of e-Safe Compliance based on ISO 27001, ensures that all the personal data is classified, discovered, usage and transfer (via Emails, USB, Clouds, IM, shadow websites etc.) of the classified data is audited, and potential breaches are reported. The reports identify the individuals or the subjects affected along with the risks imposed because of this breach.

2.3 PSEUDONYMISATION/DATA PROTECTION AND RIGHTS MANAGEMENT

e-Safe Compliance implements the protection component of the DCAP module for pseudonymisation using persistent universal encryption. It protects personal data in images and documents. It ensures that the images and documents containing personal data not only remain encrypted at rest but also remain protected during transit over an electronic network, either internally or externally. In addition to that, it allows the data controller or processor to define who can have access to the image or the document using right click options available in the mouse.

Furthermore, in the event of portability of personal data, either between two controllers, or two processors, or a controller and a processor, the receiving entity can use (view, edit, print) the protected images or documents by downloading e-Safe Compliance Rights Management iOS/ Android apps from the Apple Store and Google Play Store respectively and install on their mobile devices.

2.4 EARLY IDENTIFICATION OF RISKY BEHAVIOUR

e-Safe Compliance has a User and Entity Behaviour Analytics (UEBA) module that generates risk reports. This module applies advanced models to the data to find ‘new types of behaviour’ and changes to ‘usual behaviour’. In determining changes in behaviour, the system looks at what the user’s peers are doing as well as the users themselves, to avoid false alerts. The module identifies 40 different types of user events such as use of a new application, device, printer or network, use of shadow applications and URLs, frequent violation of rule or rules in a short span of time etc. as potential risks.

On the basis of these events the module produces actionable risk reports for DPOs or the information security team. These reports detail those users who are potential risks, and why, through behaviour analysis of users and their peers. The report also includes easy to understand explanations and scores for each reported user. Using these reports and based on risk scores of the individuals, DPOs or information security teams start monitoring the potential risky users closely to avoid any breach of personal data in the future.

2.5 NOTIFICATION OF DATA BREACH IN LESS THAN 72 HOURS

e-Safe Compliance helps organisations to avoid the penalties imposed in the event of any data breach. In case of any data breach incidents, a decentralised approach and the dual reporting feature of the integrity management workflow helps to reduce the time to identify and report such data breaches. The reports produced, identify the individuals or the subjects affected along with the risks imposed because of this breach. Hence, e-Safe Compliance helps the controllers or the processors to comply with the timeline of 72 hours and to avoid heavy fines, set in GDPR, by notifying about the breach to Data Protection Authority (DPA) and the affected individuals.

3 CONCLUSION

e-Safe Compliance’s subscription-based model with R&D as a core, ensures that technical safeguards must evolve as required. On the other hand, data controllers and processors are much better prepared to comply with GDPR if technical safeguards are properly applied in combination with physical and administrative safeguards.

4 REFERENCES

1- https://www.privacy-regulation.eu/en/4.htm
2- http://www.eugdpr.org/gdpr-faqs.html
3- https://www.privacy-regulation.eu/en/
4- https://www.scmagazineuk.com/byod-the-balance-between-achieving-efficiency-and-avoiding-gdpr-fines/article/646543/