GDPR

Preparing for the EU General Data Protection Regulation

The EU General Data Protection Regulation (GDPR) came into force in May, 2016 and B2C businesses operating in the EU (and even post Brexit UK) have until May, 2018 to ensure their compliance to the requirements set out by this new customer data protection regulation. With fines as high as up to four percent of the annual revenues, organisations are left with no option but to rethink their data management strategy.

In its broadest sense, GDPR implementation will offer customers improved control over their personal data. The implementation of GDPR will transform the way businesses manage data and run analytics projects. What's more, the regulation also gives the power back to the 'owner of the data', allowing customers to determine who may store and use their data. This will create a new focus for companies as they will serve the role of 'data custodian' and will be required to ensure that the data is accurate and up to date.

A whitepaper published by the collaboration of AvePoint and Centre for Information Policy Leadership reports that nearly 50 percent of organisations have not taken decisions regarding how to optimise their data management policies to ensure compliance to GDPR and almost 30 percent do not have additional resources available to embrace the change.

We have started to see that the fraXses platform being used for the management of customer data, allowing the multiple silos of data stored across an organisation be federated so that these data sources no longer remain as silos and accurate data management can take place.

The legislation means that Chief Information Officers need to take responsibility optimise the data management infrastructure and policies of their organisations in order to ensure compliance and avoid hefty non-compliance fines.

While this change in data management infrastructure may require additional investment in new tools and technologies, such as the fraXses platform, developing the right mind-set is equally important. Businesses also need to create a data-driven culture that supports and facilitates data protection not just because it is a regulatory requirement, but also because it is the right thing to do to acknowledge and appreciate your customers’ trust in your products/services.