GDPR: A NEW PRIVACY FRAMEWORK TO ALIGN WITH EFQM

BY: XAVIER RUBIRALTA COSTA

EXPERT FROM THE EXCELLENCE NETWORK AND PROJECT MANAGER IN THE SECURITY AND PRIVACY OF INFORMATION AT THE AUTONOMOUS UNIVERSITY OF BARCELONA

The aim of this article is to present the key points of the General Data Protection Regulation and their impact on organisations. Opportunities and challenges derived from this new European regulation are analysed in relation to the EFQM Model. GDPR came into force on the 25 May 2018.

Privacy scenarios have been reinforced with the Regulation (EU) 2016/679 of The European Parliament and of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

This regulation is oriented to protect citizens' privacy rights and their freedom. The principles of the data protection are lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability.

The GPDR introduces substantial changes to previous data protection regulations:

- It will enhance harmonisation in privacy across all EU member states.

- Territorial scope will be increased with extraterritorial applicability because all organisations that have any type of personal data within EU countries need to comply.
- Consent conditions are strengthened.
- Accountability is a pillar of GDPR therefore data and technology governance are part of the right approach.
- The right to access applies to associated personal data and the right to be forgotten includes erasing personal data and halting personal data processing.
- Data portability allows data subjects to be provided with their personal data upon request in a format that facilitates transmission to another data controller.
- A breach must be notified to supervisory authorities and to data subjects, within 72 hours of the breach identification.
- Privacy by design includes data protection controls and measures throughout the complete design life cycle of processes and systems.
- The regulation is risk focused and Data Protection Impact Assessments must be performed (DPIA).
- Data Protection Officers (DPO) should be nominated to perform this role.
- Penalties can be applied to data controllers and data processors. Organisations face large penalties, up to €20 million, or up to 4 percent of the organisation's total worldwide annual revenue.

Any organisation that manages personal data is a data controller. This data should be managed by their own employees or by designated data processors, usually third-party organisations. A data subject is any person whose personal data is detained by the organisation.

The protection of personal data is relevant in any organisation because people are a key element. Data subjects appear in the third criteria of the EFQM Model but customers and most importantly stakeholders are also people. Now is the right moment to reflect on privacy and the approach used to protect personal data just when organisations need to know more about their clients and interact more with them. It seems that data protection and customer experience are on opposite sides. Furthermore, the border between the professional and personal life of employees is disappearing.

Finding the right balance between respecting privacy and deepening relationships and mutual knowledge is a real challenge. Succeeding through the talent of people and adding value for customers are two key Fundamental Concepts directly affected by this privacy issue.

Outstanding organisations who have implemented the EFQM Model have their activity in healthcare, education and social services, which are areas where personal data is a high

sensitive issue. Behavioural profiles are also considered sensitive data.

GDPR is clearly risk focused. The first step is to identify and assess the level of risk that personal data is at. According to this evaluated risk, organisations are accountable for establishing appropriate measures to protect data. And they must be able to prove, that the risk assessments have been done and the measures have been adopted, to the supervisory authorities and in some cases for court litigations. In some high-risk cases, a Data Protection Impact Assessment must be done. With this in mind, organisational capability to deal with this risk aspect should be developed within all the spheres of the organisation and obviously privacy and reputation should be considered.

This regulation is as an important piece of the legislation body but not the only one. In the Information and Communications Technology (ICT) environment, the legislation is quite complete and it regulates different issues (telecommunications, digital services, critical infrastructures, digital signature, etc.). There are also specific sectorial regulations: financial, healthcare, pharmaceutical, etc. In the European Union, the regulation is quite similar and laws like the GDPR are contributing to this common body of legislation, but organisations that operate globally must deal with a complex heterogeneity of legislations. The protection of citizen's privacy rights around the world can vary widely from country to country. Privacy can be understood as a subset of confidentially which is one of the three pillars of information security. Protecting the intellectual property of organisations and avoiding data leakage requires similar measures to that of protecting privacy. Common approaches can be used and efficiency allows betters results with less resources. All recommendations state that a mutual support between data protection and cyber security is the right strategy to follow and should be aligned with partners and other stakeholders.

The short time in which data breaches must be notified to supervisory authorities is a real handicap. It is a clear case of where managing with agility is needed. The number of cyber incidents is growing and most of these compromises involve personal data. This agility in the notification requires mature procedures, skilled incident response teams, tools to detect attacks and data leakage as well as staff awareness and education. In the case of extremely sensitive data, the customer or citizen must be notified of the compromise of his or her data. He or she is the "owner" of his or her data and they alone decide what can or cannot be done with it.

In any organisation there are third party companies delivering services and managing the personal data of the main organisation. These partners must be equally accurate and observe all the policies related to data protection. If not, the accountability and reputation of the organisation could be put at risk. Policies are key elements to be established and observed internally and externally.

The Data Protection Officer is the person who has to orchestrate the data protection within the organisation. The GDPR clearly defines this leading figure. The Chief Compliance Officer (CCO) is another role which has a strong relationship with the DPO. The CCO is primarily responsible for overseeing and managing regulatory compliance issues within an organisation in a wider scope.

No doubt there will be litigations as a consequence of customer or even employee claims related to their personal data. Developing a forensic readiness strategy is a recommended preventive approach for excellent organisations. Forensic readiness could be defined as the ability of an organisation to maximise its potential to use digital evidence. To take the right protection measures is not sufficient, organisation must have digital evidence to prove in court that everything has been done correctly. Delaying evidence gathering until the appearance of litigations is a bad strategy. When adapting processes, procedures and information systems to GDPR, it is the ideal time to include the necessary evidence collecting processes. A key element for this is to obtain the consent of the citizen or customer for an organisation to manage his or her data. Without being able to prove this consent, you are not allowed to manage his or her data.

In previous regulations, periodic audits were in place but the GDPR's philosophy is based on continuous assessment and establishes regular control systems where the RADAR approach would be useful. Because organisations and their environments are constantly changing, risks evolve and protection measures have to be constantly adapted to new scenarios.

Big Data, Artificial Intelligence, Cloud services, Mobility, Internet of Things and Bring Your Own Device (BYOD) are technological paradigms where personal data is present and it should be properly protected. They offer huge opportunities for organisations to improve their products and services where personal data is at risk if it is not sufficiently protected. In this innovation, process creativity could be used to balance risk and opportunities. Privacy should be present in any project based on these technologies from the beginning. That is known as privacy by design. It is a similar concept to security by design. Social media is a complex but essential arena where organisations must be present and which is a key element in their reputation. Organisations have to deal with individual opinions which should be answered quickly and thoroughly.

Data protection should not be seen as a burden or a new bureaucratic obligation. It is a clear factor of differentiation of an organisation in the relationship with all groups of people with which they are involved. It is also said that privacy is threatened because of all these technologies, strong regulations like this contribute to ensure rights and freedom to EU citizens, and it is an opportunity to homogenise personal data management in

Este documento ha sido descargado de la web del Club Excelencia en Gestión: www.clubexcelencia.org