

COLLIBRA

Data Governance: Way to GDPR Compliance

FELIX VAN DE MAELE,
CO-FOUNDER AND CEO

IN MY OPINION



BY OZAN KARADUMAN, PARTNER, GÜN + PARTNERS

The General Data Protection Regulation (the “GDPR”) came into force on 25 May 2018. Although a two years grace period was granted to data controllers for complying with the GDPR, it was only at the week of the May 25th that we saw our mailboxes full with new privacy policies drafted in accordance with the GDPR. These last minute privacy notifications did not come as a surprise; the GDPR introduced new obligations which required most businesses to readjust their processes and new challenges to overcome.

Business in and outside of the EU (due to the expanded territorial scope) are continuing their efforts to comply with the GDPR and getting assistance from law firms, IT firms, data management firms and also from new technological solutions to overcome the challenges of the GDPR.

This article intends to briefly examine some of these challenges and some of the solutions adopted by the business to comply with the GDPR.

Data Inventory

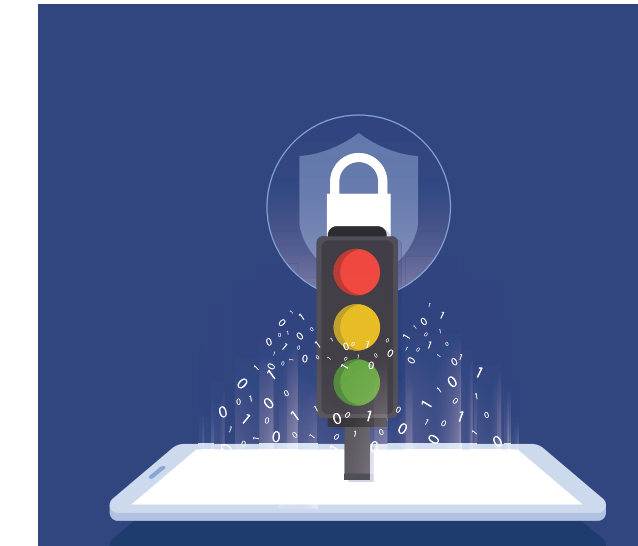
If a business wants to comply with the GDPR, the first thing that it needs to do is to be aware of its personal data activities. For that purpose, businesses prepare a personal data inventory showing the activities where personal data is processed, the purpose and the legal basis of the processing, the data subject category, recipients of data, transfers abroad, etc.

Data inventories are particularly important for the accountability obligation under the GDPR. The GDPR sets forth high accountability standards. This is very important

especially for the data controllers and processors which are not used to complying with complex privacy rules. In a nutshell, the accountability standards under the GDPR require the data controllers and processors to be able to demonstrate their compliance with the GDPR. It may seem a straightforward obligation but it is not. It would be very difficult, if not impossible, for a data controller to comply with this obligation without having an organized view of its data processing activities. This is where the data inventories come into play in this regard; they enable the businesses to have a control over their processing activities.

Data inventories are useful for the observation of data transfer activities as well. Data transfers outside European Economic Area are regulated under the GDPR. The GDPR does not want the personal data to be transferred to third countries unless certain specific conditions are met. The reason behind this restriction is to avoid the undermining of the level of protection provided by the GDPR when the personal data is transferred to third countries. Data inventories show the countries where the data is transferred and therefore enable the businesses to keep a tab on their data transfer activities.

There are various other uses of data inventories, though preparing a data inventory is not an easy task. In practice, businesses require the assistance of lawyers and/or IT and data management consultants for preparation of data inventories. There are also newly developed software for preparation of data inventories. There are quite a number of businesses which prefer to employ these new technological tools to prepare data inventories. The features of these tools may differ; some of



**VARIOUS DATA PROCESSORS HAVE
READJUSTED THEIR SYSTEM TO BETTER
COMPLY WITH THE GDPR ALLOWING THE
DATA CONTROLLERS THAT USE THEIR
SERVICE TO HAVE BETTER CONTROL OVER
THE PERSONAL DATA**



them facilitate the phase of asking questions regarding the processing activities by providing various pre-prepared questions and preparing reports based on the responses given to those questions. Some of the tools claim to be able to sort out the personal data within a large cluster of big data and thereby help in preparation of a data inventory. However developed such tools are, they still require human input in order to finalize the data inventory; the questions posed by the tools must be responded by the employees or the consultants of the data controller and the employees or the consultants of the data controller must give input in relation to the parameters to be used by the tools that automatically sort out the personal data from the servers of a data controller or to analyse the output generated by that input. It would not be a far-fetched estimate to say that these tools will be supported with artificial intelligence and machine learning in the close future, which will bring them closer to being self-sufficient for generating data inventories. For the moment, a data controller needs to employ its own officers or consultants in addition to the available tools to prepare a data inventory.

Data Protection by Design and by Default

Data Protection by Design and Data Protection by Default are concepts that are considered good practices in the privacy spheres for a long time. The GDPR accepts these concepts and requires the controllers to adhere to these concepts with its Article 25.

According to Article 25 of the GDPR, the data controller implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects and keep the data secure. Data controllers shall also implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.

These are important and high level standards; these principles require the data controllers to review their processing structures in whole and readjust them in a way that -by default- the personal data is collected and processed only to the extent required for the purpose of processing and is accessed by third parties only to the extent required for the purpose of the processing.

This is also an area where human input is used together with newly developed software. There are now a number of software that allows the data controllers to pseudonymize or anonymize personal data. Furthermore, various data processors have readjusted their system to better comply with the GDPR allowing the data controllers that use their service to have better control over the personal data, providing them with a number of options including but not limited to the ability to delete or modify and to have access to the personal data of the data subjects and to log the activities related to personal data so that the accountability obligation is met. Some of the data processors also allow for the option to inform the data subjects and getting consent where necessary. Furthermore, data processors are also increasing the level of security and providing more options for data breaches. The level of compliance with the GDPR will also be a decisive factor for the data controllers when choosing their data processors.

A Final Word

The GDPR sets forth very high standards for data protection which can be challenging for data controllers. This is due to the technological developments which allow easier procession of personal data in high scales. The same technological developments also provide some solutions for responding to these high standards. For the time being, human input is also required for most of these solutions. However, together with the developments in the AI and machine learning, we will also see technological solutions which do not require human input for some of these solutions. **CA**

