GDPR AND INFORMATION SYSTEMS AUDIT

GDPR

The expansion of Internet and technologies was of tremendous help for globalization as we know it nowadays. Today, sharing information on the Internet takes more than a click, it includes sharing our identity; identity which can be risk. During the first years of the expansion of the Internet, semiconductor storage chips then floppy came to facilitate storing personal data for some, financial institutions saw an opportunity linked to data.

In fact, the World Wide Web (WWW) was still under obsolete forms in 1990; the world still has a long way to go before even thinking about data management and vulnerabilities. As the Internet grows, the trend of computed tools expands and a new dilemma arises; the ethic behind data storage. In an intent to protect citizens rights and safeguard users' personal information, government officials implement the General Data Protection Regulation (GDPR) as a solution to the ongoing challenge and complexity of user data usage and storage. General Data Protection Regulation (GDPR) is a rule instituted by the European union in 2018.

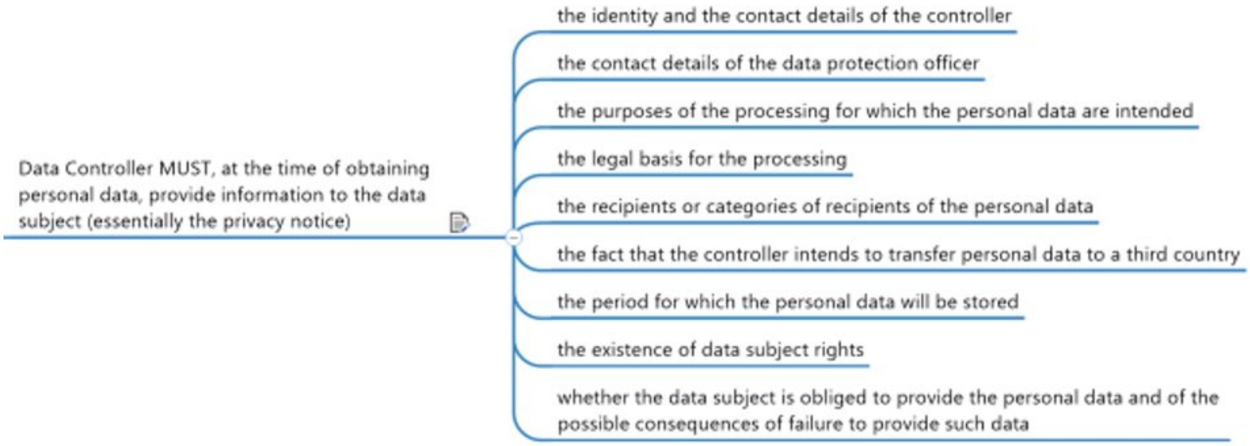
Even though the law came into action in 2018, GDPR policies have however been planned for many years before its application with it an initial publication made in Mai 2016. The General Data Protection Regulation (GDPR) was firstly intended to protect data stored by organization - for paid or unpaid services - ; but several processes and rules had to be strictly followed by companies.

The very first point GDPR made clear for the companies and enterprises processing user data is that its policies go beyond the frontiers of the European Unions and its Economic Areas. For instance, a US company which processes personal data from users living in the European

Union must absolutely complain to the regulations under GDPR. This point in highly important as it pushes US companies to create different processes and maintain different types of regulations when dealing with their internal and external information systems and databases. In the area of e-commerce for instance; no clear rule has been established, by the US government, regarding the necessity of a privacy policy statement. Furthermore, companies in the US, are not required elaborating publicly what they do with user data.

GDPR, allows users to ask for their data from companies. While some providers like the social media giant Snapchat allow its users (even those outside of the European Union) to get access to their data, many do not intentionally follow the same pattern in the US.

In the European Union, all companies, are required to provide users data upon requests from the users. GDPR goes beyond by allowing user the right to know what is being done, with their data. Also, under the ruling, European users have the right to know why analysis or research are being made with their data. It is important to note that companies are required to give users' data for free to a user who ask for it. (Please see the picture below for a better insight into user rights under GDPR)



Data Controller MUST, at the time of obtaining personal data, provide information to the data subject (essentially the privacy notice)

- the identity and the contact details of the controller
- the contact details of the data protection officer
- the purposes of the processing for which the personal data are intended
- the legal basis for the processing
- the recipients or categories of recipients of the personal data
- the fact that the controller intends to transfer personal data to a third country
- the period for which the personal data will be stored
- the existence of data subject rights
- whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data

This Photo by Unknown author is licensed under CC BY.

Another point that companies in Europe but also all foreign companies dealing with European users must comply under is to allow users to be “forgotten” if they ask. Under this close of the law, a user can ask companies to delete all the information collected about that particular user. In the US the user sometimes can ask to unsubscribe from a marketing email under the CAN-SPAM Act of 2003. Under the CAN-SCAM act, marketing emails have to possess a visible unsubscribe option, be not deceptive and label relevant information according to their headers. Both the GDPR point to allow users to be “forgotten” and the CAN-SPAM act give control to user over their personal information.

A prolongation of the rights to ask one’s data under the General Data Protection Regulation means that user can request the data in the aim to transfer them to another company. To put this into action, if someone wants his or her data to be transferred from one vendor to another, the company the request is made to shall do as the user asks and allow the transfer.

Beside users' rights, the General Data Protection Regulation (GDPR) requires consistent rules to secure user information; again, all companies have to comply to those rules without exception.

Under GDPR, data shall be under protection since their very first storage. Companies shall be sure to implement the relevant encryption and security systems in order to prevent the breach of any personal information. It is therefore e logical that GDPR oblige enterprises to possess relevant computer information systems that not only allow efficient data protection but also document system administration processes and issues for future audit.

Another important branch of GDPR obliges companies to inform users of any data breach that happens. In fact, any data breach must be notified to the Autorité Nationale de Protection. In order to manage data breach efficiently, under GDPR, companies shall possess an internal a Délégué à la Protection des Données (DPO), a team responsable for data protection.

The team responsable for data protection shall make continuous checkups. Not only the team has to make sure the company follows the requirements of the GDPR ruling, but they must be full transparency and be impartial even if there are employees of the company. In addition, of auditing themselves, companies shall undergo a thorough evaluation of a new product or services before it is launched to the audience.

The General Data Protection Regulation (GDPR), the ruling, impacted all institutions, in Europe, functioning with user data. Countries affected by GDPR are Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Channel Isles, England, Northern Ireland, Scotland, Wales and Sweden. In addition, of those territories is added Iceland, Lichtenstein, and Norway.

It’s of tremendous importance to follow GDPR rules and be aware of when they apply to companies. If not complying to GDPR laws, organizations face sanctions and fees up to 20 million EURO or 4% off the company’s profit. However, the authorities in charge of implementing the rules forgive the first in fragment made by companies. It is to notice that regular audits can be made in order to make sure that regulations are followed as required.

On the other side, GDPR is not all user rights and rules to enterprise. The General Data Protection Regulation possesses advantages to companies. By following the requirements imposed by GDPR, companies are able to keep a transparent record and have the highest security systems to protect not only the users' data, but also their own.

Now that a deep understanding of GDPR has been implemented, let’s take a look at Information Systems audit, it processes requirement and demand in the US but also in Europe.

AUDIT PROCESSESS

To make sure data is secure, that companies respect users’ rights and governments’ laws, audits are demanded and vastly insured in the US. The main goal of audit is to verify that rules are respected. Moreover, it helps to identify, reduce or eliminate issues before they bring bigger consequences. In an effort to reduce economical fatalities like corruption the US government put in place regulations that companies must abide to in order to lawfully continue to provide their services.

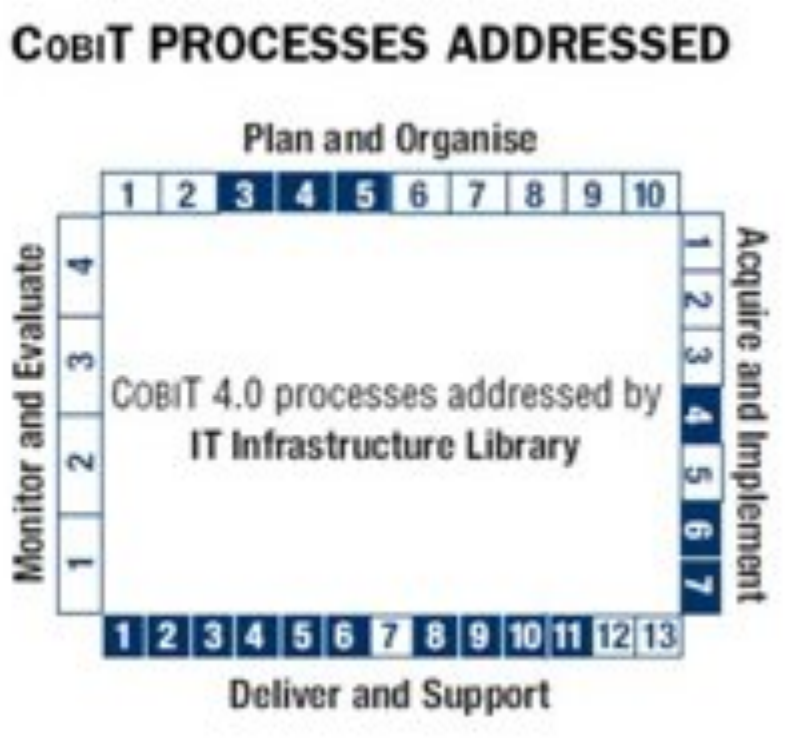
While it may be widely taken that Information System audit follows the same pattern as financial audit, it is important to point that Information Systems audit, in the US, is not required to cover the examination of internal processes.

The very first phase of audit is planning. Planning permits to implement the objective of the mission. It gives an exhaustive list of points to cover, clears up an evaluation of the tasks in accordance with auditors' resources and material is made before anything else. This phase goes in three directions: Responsibility, Authority and Accountability.

In the Responsibility section is made the Audit Charter. The Audit Charter, is the main document tracing the aims of the mission. Authority is to make sure the responsible and entities in control are clearly noted and known; this section attribute to auditors the right and privilege needed to carry the audit to a positive outcome, but also gives a clear understanding of what is expected of the entity being audited. The goal is to make process as smooth and transparent s possible. Lastly, Accountability come into place to compel the first step of the audit. Accountability comes into place to verify that the Audit charter, with transparency and accuracy not the tasks and actions and agreements needed to carry the audit.

Phase two (2) of the audit process is to assess risk, and analyze processes related to business. In fact, using risk assessment to lead audit is a current trend followed by numbers of institutions as this method is adaptation. The importance of this phase resides in the fact that it helps auditors with choosing between compliance testing and substantive. However, this method not only supports itself on risks, but also include the use internal processes and control operations.

Phase three (3) of the audit is the actual actions related to audit. During this phase, auditors with perform review and revision in accordance to the plan and requirements outlined in phase one (1). During review, auditor collect the information they need; including relevant proofs. It is to note that documentation is made also during this phase as auditors go through files and systems. This phase of the process is simplified in the Control Objectives for Information and related Technology (COBIT) implemented by ISACA (the Information Systems Audit and Control Association) and ITGI (IT Governance Institute) (view image below).



This Photo by Unknown author is licensed under CC BY-SA.

The last phase of the auditing process will be Reporting. After gathering evidence, documentation and going thorough processing and systems; auditors convert the outcomes of the examination and deliver a thorough document (report).

Resource

https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

https://en.wikipedia.org/wiki/Information_technology_audit