General Data Protection Regulation

Ibrahima BA, *Student engineer RT 5, UTT,* Aurelien DIAS, *Student engineer RT 5, UTT,*
Arnaud FOURNIER *Student engineer RT 5, UTT*

***Abstract*—The development of New Information and Communication Technologies (NICT) has made our society more and more digital. Companies are increasingly using the personal data of users as part of their business. The protection of this data is therefore essential. This was initiated in France by the "*Loi Informatique et Libertés*". The first data protection act at a European scale is the European Directive 95/46/EC which defines the principles to respect when a company is collecting, processing and storing personal data. On May 25, General Data Protection Regulation (GDPR) will supervise the data protection by radically changing the rules of the game for both companies and users.**

***Index Terms*—Personal data, Digital, law, Company, clients, Users, Right, Compliance.**

I. Introduction

GENERAL Data Protection Regulation is the most important act in the protection of the online private life for the last 20 years and since the CE directive on the personal data protection in 1995. This comes to fulfill a major gap in data privacy that has become more visible in the recent years with the booming use of personal data by companies. Indeed, with the improvement of computational power, the expansion of the Internet and the apparition of smartphones, user's personal data are constantly exposed and risks are increasing in terms of privacy violation, be it from attackers or by the companies themselves. We all saw it on the media, and cybercrime has been skyrocketing from year to year so there was a need to protect us against it at a global scale.

In France, the spirit of GDPR is not new. Indeed, in 1978 the "*Loi Informatique et Libertés*" was established. This law derives from the 1974 SAFARI project (computerized System for Administrative Files And the Repertoire of Individuals) that the French government wanted to set up at the time. Its purpose was to create an automated administrative file from the social security number. French people were strongly opposed to this project, so the government was forced to adopt the LIL instead. It is a French law that regulates the freedom of processing personal data and makes it possible to protect the citizen when an organization or an enterprise want to collect, preserve and use certain citizen's personal or sensible data.

This law of 1978 also created an independent data protection authority, the National Data Processing and Liberties Commission ("*Commission Nationale de l'Informatique et des Libertés*", CNIL). In 2004, the law has been subjected to a major update, and only the first article has been preserved. Yet the territorial application of this law was limited to France uniquely, that is why a European Harmonization was needed. The first European directive (95/46/EC) about data privacy has been established on 24th of October 1995 and concerns the protection of individuals regarding the processing of their personal data. However, since then, public awareness, technology, and the access to the Internet have been growing wide. Many companies do not fully respect the rules due to the complexity of managing and controlling data, and also probably because the administrative penalties are often negligible compared to the profits of certain big companies. This is a real problem because they have the biggest processing capacity and the highest influence, so they are the most exposed to attacks and abuse. For these reasons the current regulation does not seem to be sufficient and adapted anymore. That is why the GDPR has been set up by the European Union.

We organized the remaining of the paper as follows: section 2 presents the principles of the GDPR and section 3 introduces some of the main concepts brought by this regulation. Then in section 4 we discuss the role of Data Privacy Officer in the company and in section 5 we talk about the Data Protection Impact Assessment as defined in the GDPR. In section 6 we will focus on the role of the supervisory authority and in section 7 is about the different levels of maturity of companies when facing to the GDPR. In section 8 we conclude our paper.

II. Principles of the GDPR

A. Scope and objectives

GDPR stands for General Data Protection Regulation, it is a European reference for personal data protection of all European citizens. It will be applicable on May 25th, 2018. It contains 99 articles that where published in April 2016. This gives 2 years for companies to be in conformity.

The main goal of the GDPR is to bring legal power to force companies to respect the rights of citizens concerning their privacy, but also to bring more transparency on how companies collect, process and store personal data.

For companies, the main stake is to make their processing more secure, and to keep track of every risky treatments so at all time they know what kind of data is collected and processed, the responsible person associated with it and the purpose of the operation.

B. Changes for companies

1) Who is concerned: Concerned companies include companies processing personal data of European citizens. Therefore it can be companies, associations or public organizations whose headquarters are not in the EU but which operate in the EU. Subcontractors may also be concerned by the regulation.

2) Processors and Controllers: A processor is a natural person, public authority, agency or other body which processes personal data from the controller. A controller is a person, public authority or an agency that determines the purposes and determine all processes on personal data.
In order to distinguish the difference between a controller and a processor, we can take the example of a company that collects data such as a bank which open accounts for their clients and another company such as an enterprise that stores bank's data in a datacenter. In that case the bank is the controller and the company which owns the datacenter is the processor.

3) Obligations: The regulation changes how companies will work. Companies will have to inform their clients of what kind of data they collect, why and for how long they will keep it. To achieve these goals sanctions have been strengthened a lot so that even the biggest companies will have to comply with it.
They will also need to list every processing with high risks and to analyze the impacts through the writing of Data Protection Impact Assessments in order to know if and where there are security points of failures.

C. Difficulties

The main goal of the GDPR is to enforce human rights by creating a data portability right. For companies like GAFAM this is a huge change of habits. They will need to change the way they organize personal data in their information system.
Most of the companies will not be ready when the GDPR will enter in application and the reasons are money and skill. For a company that treats a huge amount of data it is really costly to implement scaled measures that will be efficient in branches, departments and subdivisions.
Smaller companies will not systematically have the appropriate skills to implement technologies as advanced as anonymization. The CNIL is aware of all these problematics and in the case where a company is not conform with the GDPR they can decide if they give the a fine or not. Of course it is depending on the company willingness.

III. Main concepts Of GDPR

A. Protect citizen rights concerning their personal information

Sensitive personal information or personally identifiable information, as described in the Article 9 the GDPR, is a data that can uniquely identify a natural person directly or indirectly like an IP address, name, localization, license plate, biometrics, ethnic origin, political opinions, religious and biometric data. According to the regulation any informations relating to an identified natural person shall be prohibited to respect and protect private life of data's owners. In the following every use of the term "*personal data*" will refer to the definition presented in Article 9 of the GDPR.

We can also mention the Article 10 which states that the processing personal data relative to criminal sentences or offenses must be supervised by the public authority and only the latter can keep a complete registry of this data.

The GDPR emphasizes on the rights of European citizens, so they can demand companies to respect their privacy in case this represents an issue for them. These rights are listed below:

1) The right to be informed: One has the right to be informed about everything that happens with his/her personal data, what for they are used, how to access them, how to modify them and that this data must be accessible at all times when asked for.

2) The right to refuse to become a targeted person.: As a citizen of the EU one can refuse to be a targeted person, which means one can refuse to have his/her personal data being processed by a company or organization.

3) Data portability: One have the right to move his/her data. Therefore one can transfer his/her data from one provider to another in an easy and quick way.

4) The right to be forgotten (the right to erase data): Another important right is the right of erasure also called the right to be forgotten. The person concerned may therefore request the erasure or deletion of his/her personal data.

5) The right to restrict data processing: According to the GDPR, a person has the right to restrict the processing of personal data in various circumstances (example: incorrect processing of data).

If these rights seem pretty on the paper, it is still unlikely to observe that tomorrow companies will have to handle thousands of request for the application of these rights. Indeed, as we said most of businesses and applications relies on the processing of personal, thus demanding to be forgotten or to restrict the processing will simply make the use of the service impossible or inconsistent.
Therefore in practice, most of the people will keep on going as it has always been, and nobody will ever complaints except in rare specific cases.

B. Privacy By Design and by Default

1) Privacy By Design: This is a new concept presented in the Article 25 of the GDPR. The main objective is to protect personal data processed in new softwares, applications and every on-line-based products.
The problem is that companies are not constantly considering privacy and security during a product's conception, because it is costly and time consuming. Currently, neither the EU rules regarding Data Protection nor laws like "*Loi Informatique et Libertés*" in European countries contain a similar requirement. This leads to huge breaches that can compromise confidentiality and integrity of people's data.

The GDPR will guarantee that the companies will think about and promote privacy and data protection from the conception. For each service that process personal data all the decision makers must implement security measures in order to protect this data. This concept is important for companies that process a huge amount of personal data because it forces companies to increase the security level of their applications, thus reducing the risks of data leaks.

2) Privacy By Default: This concept has been introduced for applications and services that are already in production.
It forces companies to think about privacy and data protection for their products already in use. Many services were on-line before the GDPR and many of them are not ready for the requirements of the GDPR. Therefore privacy by default concept will force companies to patch those services in order to comply with the GDPR.

The implementation of this concept guarantees that all the personal data required for a treatment is used, and apply through the quantity of collected data. It guarantees that all the personal data collected are unattainable for some people that do the treatment.

3) Application: In the future companies will always have to think about privacy aspects during the development of applications. This might be constraining but it is essential for respecting citizen's rights. The fact that this concept also applies for old softwares and services adds even more constraints but without this requirement, companies would certainly have continued to violate the concept of privacy.
Data controllers must implement measures not only on a technical aspect but also on a organization level to ensure that personal data is used for specifics purposes that are defined by the DPO. But behind those concepts there is a technical aspect that companies must not overlook, which includes technologies like pseudonymisation, randomization and encryption.

C. Accountability

The notion of accountability have been introduced in the regulation. This means that a company is responsible to take all the measure to respect the regulation but also to show to an authority, the CNIL, that they respect it. To take measures, a company have to adopt intern rules, those rules are a conservation of all personal data treatment under the control of the treatment responsible, named a DPO, realize a DPIA that is an impact analysis for all the treatment that represent risks for violation of rights and liberty and adopt a privacy by design approach. According to Article5(2) accountability, the controller is responsible for the demonstration of conformity to the authority.
How can the controller can prove that his organization is conform? First, he can prove it with the first step of preparation to the regulation with information campaign, staff formation and information system security. Shows pertinents documents such as data protection policies. The following steps are to implement solutions to be conform to the regulation like pseudonymisation or data encryption and of course a DPIA. A certification could be beneficial as a business argument to attract clients. However there is no concrete interest in certification because no official standard has been defined in the GDPR.

IV. Conform and Control : The Data Privacy Officer

The new regulation introduces a new status related to data processes, the Data Privacy Officer (art 37-39). His main role will be to control that appropriate means are used to conform to the GDPR. In France, a similar role has been in place since 1978 and the Law of Information and Liberties, however the new regulation will slightly change the scope of this role. In this section we will first present the former role described in the French Law of Information and Liberties, then we will talk about the changes to come with the GDPR and finally we will discuss about how companies can cope with this new status.

A. Information and Liberties Officer (CIL)

The French status already existing in a similar role as DPO in France is the CIL. He has a total independence regarding his hierarchical superior when practicing his functions of CIL. The main role of the CIL is to diffuse a liberty and information culture in the company, using different means. For instance he can create a data privacy policy to establish rules and good practices.
The CIL also has to advise the different managers and inform them about how they should collect, process and store personal data. In fact he is a mediator and coordinator that helps decision makers to be in accordance with the law. Indeed, he must keep a registry with all the different data processings made by the company for transparency.
Finally, his role is to facilitate the communication between the CNIL and the company. For instance having a CIL reduces the amount of formalities the controller and processor have to send to the CNIL.

B. Role of the DPO

Like the CIL, the main role of the DPO is to inform and advice every employee in relation with data processes about the aspects and obligations. He will also be the main contact point with the CNIL for prior consultations, so he also needs to know every sensible processing operation and the risk associated with it. Nonetheless, the new aspect that differentiates a DPO from a CIL is the monitoring activity. Indeed, the DPO has to develop strategies for supervising security measures and must be able to present a proof of conformity via the Data Protection Impact Assessment. In order to achieve this mission data controllers and process managers must give access to all process information the DPO would need.

The position of the DPO in the company is specified in article 38 of the GDPR. He is totally independent of the process managers and controllers who must provide all the information about data processings to the DPO. He is also in charge of protecting personal data and has to handle requests for data subjects concerning the processing of their personal data.

C. Implications for companies

The article 37 specifies the conditions for companies that must designate a DPO. This includes all public organizations except courts, companies that process a large amount of data which require the monitoring of data subjects and companies that process personal data as defined in the Article 9. Other companies are not required to designate a DPO but they need expertise and coordination to conforming to the new regulation.

A DPO can be an employee or an external person, and must have a strong knowledge of data protection laws and practices. In the case of internal DPO, the designated person can have side projects as long as there is no conflict of interests with his status. For instance he can neither be a process manager nor a developer nor a data controller.

The easiest way for companies that already have a CIL will be to transfer the new role of DPO to this person. However, the simplicity of this solution has several drawbacks especially for companies with low and medium maturities. In those companies the role of the CIL is in general limited to communication and raising awareness. Most of them does not have the technical skills to perform control tasks. Therefore, this will inevitably lead to errors and misdirections. The second drawback is of course the additional amount of work such a fusion would imply.

In that case the best solution for French companies is certainly to make the CIL and the DPO work in complementarity. For instance, we can imagine the CIL diffusing and facilitating the establishment of a "culture" for privacy and the DPO regularly controlling or certifying to give a proof of the conformity.

V. Managing the risk : Data Protection Impact Assessment

A. Presentation

The new regulation demands that companies carry out a Data Protection Impact Assessment (DPIA). A similar procedure called Privacy Impact Assessment (PIA) was already defined by the CNIL and other European authorities. With the GDPR, the two terms are employed for designating the same process. The only difference brought by the European regulation is in terms of responsibility. Indeed, whereas in the past years the PIA was performed by the CNIL now it has to be undertaken by the process manager with the help of the DPO when designated.

This document is meant to be written for each processing operation ahead of its execution, in order to assess the impact this treatment will have on personal data. This approach relies on a risk analysis for any processing that can potentially lead to a violation of rights and freedom of the natural people concerned. One assessment can include several operations that are similar in terms of risks on the data. More precisely, a DPIA must be implemented by the controller when the processing falls into one of the following cases:

1) When personal data is used for evaluating a natural person via automated processing or profiling, whose result can lead to legal consequences or similar effects for the person. For instance when a company sends customized selling offers based on people's address.
2) When personal data as defined in article 9 and 10 are processed at a large scale.
3) When a publicly accessible area is subjected to systematic monitoring, like video monitoring.

These cases are not exhaustive and the regulation precises that this list can be extended by the different national supervisory authorities. Conversely, supervisory authorities such as the CNIL should also make public a list of processing operations which do not require an impact assessment.

B. Methodology

The analysis is based on EBIOS methodology provided by the ANSSI (the French agency for information systems and security). The course of action is divided into four steps:

1) Context: Describe the concerned processings in terms of nature, scope, stakes and goals, the different people implied in the treatment and their responsibilities (managers, subcontractors, service providers, etc.).

2) Measures: Identify existing measures and determine forthcoming ones. There are two types of measures: measures in order to comply with the law (the CNIL defines eleven privacy requirements) and measures for mitigating the risks.

3) Risks: The CNIL defines a risk as "*a hypothetical scenario which describes how sources of risk could exploit vulnerabilities within the scope of a threat and thus how they could enable undesired events to happen on personal data that will have impacts on the concerned people's privacy*".
The level of risk is characterized by a gravity and a likelihood.
The gravity is found by analyzing the impacts of an undesired event (loss, disclosure, corruption).
The likelihood corresponds to the threat having the highest likelihood of being triggered by a source of risk.
This step leads to a mapping of every risk according to his level of risk.

4) Decision: This last step consists in evaluating measures and risks that are described in the PIA and in determining if improvements can be done. It is in general performed by a different person from the one who wrote the PIA. For instance it can be the Data Privacy Officer when designated in the company.

C. Facilitating the transition for companies

In order to facilitate the shift of companies towards this new responsibility, the CNIL has released a guide which comprises three documents. The first one details the general methodology presented above and the second provides a tool box with a knowledge basis for each step. The third document is a manifest of the good practices which gathers common measures for mitigating the risk. They have also developed a turnkey application which facilitates the establishment of a PIA. Its interface is showed in Figure 1.

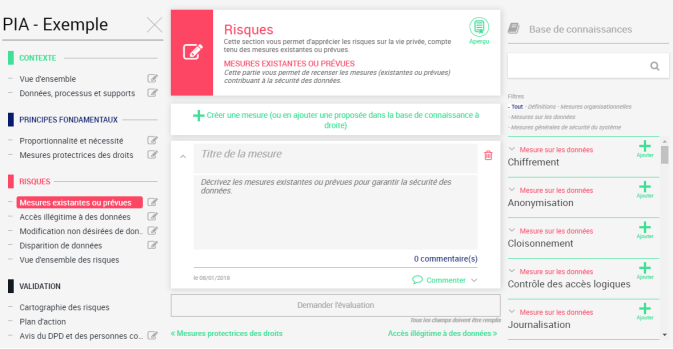

Figure 1: Screenshot of CNIL's PIA application

We can see that the course of action is set on the left and for each step a form has to be fulfilled by the user. Also in the right we can see that a knowledge database is provided with a set of examples of measures and risks with corresponding impacts and undesired events. When the document is fulfilled the step of validation can be performed by a third party person such as the DPO.
As mentioned in the CNIL guide, the PIA is an iterative process which has to be done in a continuous improvement mindset. In those situations experience is the best lesson one could have to improve. It is all the more true that companies with low and medium maturities will certainly encounter difficulties in establishing an efficient PIA at first sight.

We can see that this process requires to have some technical knowledge in information systems security because this will help to determine correctly what are the risks to assess in priority and which measures will lead to the most adequate results.

VI. GDPR Supervisory Authority

A. The CNIL

Introduced in the article 51, the supervisory authority is one or more independent public authorities responsible of watching the application of the regulation and monitoring it in order to protect the private life of a natural person. A State member of the Union must create at least one supervisory authority and according to the article 7, all the authorities of the EU have to cooperate together. For example in France there is a single authority organization named "*CNIL*" despite of some State members of the Union that do not have any authority.
The CNIL was created with the purpose of ensuring the protection of personal data to protect privacy and individual or public freedoms. The CNIL has the mission of informing individuals of their rights accorded to them by the "*Loi Informatique et Libertés*". CNIL provides some practical and educational tools to individuals and professionals for training and awareness actions, especially in the context of digital education. One of them was presented above and concerns the establishment of a PIA. The CNIL also participates in conferences, seminars, and workshops in order inform people of their rights and obligations.

B. Accompanying the Conformity

The biggest difficulty for many companies is, in fact, to know where the data are and how they can collect and transmit them to a concerned person who requested them. This is why the role of the CNIL will be to help these companies to conform.
In addition to the guide and the application presented in the last section, the CNIL has published the 6 steps[2] on its website to prepare for compliance before May 25th.

1) Designate a driver: The driver basically has the role of a DPO, but small companies are not fully compelled to designate somebody as such. Still someone has to take the responsibility of the compliance, and this might be the Information Systems Security Responsible in some cases.

2) Mapping the processing of personal data: It is important for the company to start with the inventory of the personal data processing that it implements. That is a key step for compliance with the GDPR. To achieve this requirement, it is necessary:

- To recent the different treatments of personal data.
- For the controller to know:
  - where the data is stored.
  - how long the data is preserved (archiving).
  - Subcontractors who intervene on the processing of personal data.

It is also important to know that companies that are not part of the European Union will also be concerned from the moment they process data from European citizens.

3) Prioritize: Companies will have to implement an action plan to be in compliance with the European Regulation for their future actions. So, these actions must be prioritized according to the risks related to the rights of the concerned consumers.

4) Manage risks: For processings of personal data that may entail high risks, a company must conduct a DPIA. The risk of data hacking should never be neglected. Actions must be implemented to reduce the consequences of these attacks: data access must be reduced, softwares regularly updated, data flows must be known.

5) Organize internal processes: To ensure a high level of personal data protection, companies must implement internal procedures that ensure data protection at all times. To do so, companies must take into account the following elements:

- personal data protection from conception of an application (privacy by design).
- sensitize and organize the information.
- handle the complaints and the requests of the people concerned on their new rights (access, rectification, opposition, portability, and erasing data).

- anticipate data violation: in order to notify the data protection authority within 72 hours and to the person concerned as soon as possible.

6) Document compliance: In order to prove their compliance, companies must demonstrate a complete documentation, updated regularly. As a result, this will help to inform individuals about the use of their data, to recover their consent in order to have proof of their agreement.

C. Inspecting and Sanctioning

During the control of the CNIL, computer applications are checked in order to assess whether the law is respected. The security of information systems is also monitored to ensure that all precautions have been taken. This is to prevent the data from being distorted or communicated to unauthorized people. If the law is not respected, CNIL pronounces various sanctions against controllers. These sanctions can be:

- A warning, which can be published.
- A fine.
- An injunction to stop treatment.
- A withdrawal of the authorization accorded by the CNIL.

For the transfer of personal data, companies are subjected to the countries of destination only on certain conditions. The map below[3] allows to view the different levels of data protection in countries around the world.

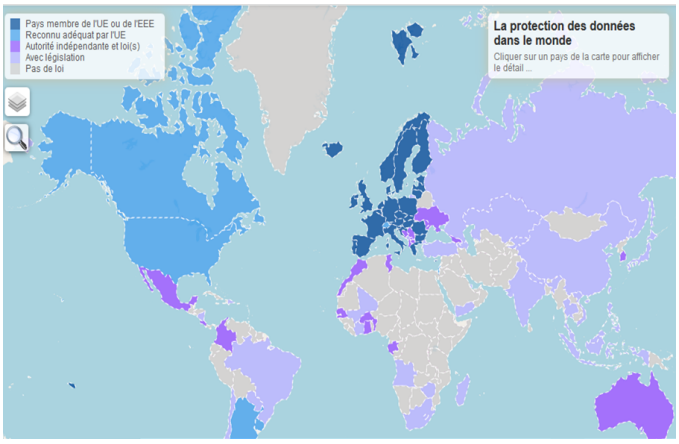

Figure 2: CNIL Data protection around the world.

Before GDPR, the non respect of the LIL "*Loi Informatique et Libertés*" or the European directive can lead to the following sanctions:

- Administrative penalties: Warning; withdrawal authorization; Injunction to stop treatment.
- Pecuniary sanctions: The financial penalties can go up to three thousands euros fine and the publication in the press of these sanctions. But currently with the modification of the "*Loi Informatique et Libertés*": the sanctions can go up to three million of euros.
- Penal sanctions: the person responsible can incur up to 5 years in prison and a fine of 300 000 euros.

Those sanctions have been incredibly strengthened on respect of GDPR. The maximum penalties expected are: ten millions of euros or 2% of the global turnover in case of non respect of the following points:

- Absence of Privacy By Design/default.
- Lack of cooperation with the authority of control.
- No notification of a violation of data protection to the supervisory authority or the person concerned.

In extreme case, penalties can even rise to reach a total up to to twenty millions of euros or 4% of the global turnover, the maximum value being chosen, in case of non respect of the following points:

- No respect of the basic principles of a treatment (sensitive data, loyalty, legitimacy, adequacy and relevance of data, consent).
- No respect of the rights of individuals.

VII. Maturity level of a company

Only few months before the application of the GDPR, some companies have not done any approach to comply with the regulation yet. In this section we will develop the maturity degree profile of organizations for personal data protection.

A. Low maturity level

Some companies have a low level of maturity and the different controllers and users are not sensible about data protection. Those companies often do not have a CIL, or the CIL function is merged with the DSI or RSSI function. Personal data security depends a lot on the security of the company's information system as well as the quality of security devices. The company is not ready for the application of the regulation and does not plan to do it.

The difficulty is to raise awareness among employees and especially among the controller. The whole success of the transition will depend essentially on this part.
The private policy and the register have to be conformed to the information system policy and the organizations should be able to demonstrate it and prove it to the authority.

Privacy by Design and Privacy by Default concepts are difficult to implement for this kind of organization. Indeed, risks management standards like ISO27005 and ISO31000 are not an efficient way to comply with the regulation. To ensure a valuable transition the DPO must work with the RSSI to combine technical and non technical aspects of the GDPR.

B. Medium maturity level

A company is in a state of medium maturity level when there is a CIL. The CIL must raise awareness among all the controllers, directors, users and subcontractors. During the conception of products, data protection is disregarded. The organization already has a plan and starts to make awareness campaigns inside the company but it is still not ready to implement and to comply with the regulation.

The nomination of a DPO is one of the biggest addition of the regulation and organizations at this level of maturity have not designated one. Moreover, a processing operations register is required for all treatments on personal data. It must record how long the data is preserved and how it can be returned to the client. This point is not new for French companies but now the sanctions will be harder in cases of negligence.
However, data governance is a big process to deal with and there is no doubt that this will be a difficulty for some organizations. Concerning the integration of the security, the difficulties are the same as for organizations with low maturity level.

C. High maturity level

Conversely to the low and medium maturity levels, high maturity corresponds to companies which have already anticipated regulation and that have a plan to implement before the application of the GDPR. Those organizations have CILs who have raised awareness campaigns and formations in the company. Every in-development project integrates personal data security.

The data governance aspect is approximately done by this kind of organizations and they will just adjust some changes to accredit the governance. The challenge is to give the DPO function to someone who does not have conflicts of interest with the activity and who does not hold currently others functions as CIL or a DSI or a RSSI. It is important to underline this is not forbidden but simply not in the spirit of the regulation.
Risks management ISO standards, MEHARI and EBIOS methods and pentest audits are additional elements to prove and to ensure data privacy. Until the application of the regulation, organizations goal is to comply with the GDPR and to be certified to prove to their clients that they are conform.

Organizations must try to maximize the maturity level to conform to the GDPR but this will have repercussions. The workload of the RSSI will increase, technicals solutions for providing data protection will be implemented by him.

VIII. Conclusion

Finally, we note that the spirit of GDPR is not new in France but dates from the law of 1978. Nevertheless, this regulation standardizes the good practices in terms of data protection and brings lawfulness in order to force companies and organizations to respect people's rights in terms of privacy.
If the GDPR may be considered a legal and organizational constraint, it is also a perfect opportunity for many companies to take the control of their data. With the explosion of data processing we have seen the emergence of many companies whose business activities represent a major risk for data privacy.
In that sense the new regulation goes further than previous laws: it has a global impact because every company in the world that processes personal data of European citizens will be concerned. It forces businesses to secure personal data and to be transparent about their treatments via the DPIA.
The Data Privacy Officer will be the corner stone of this regulation because on one hand he will help companies to conform and on the other hand he will control the respect of the application of the laws. Besides, sanctions have been strengthened so they bring more incentives to companies for taking the necessary measures.
One of the most important challenge for companies of low and medium level of maturity is to find solutions to comply with the regulation and to implement data governance and supervision. Another challenge for organizations is to provide personal data security in addition to the information system security.

References

[1] Denis VIOLE, "Maturité d'entreprise et plan d'action pour la mise en conformité avec le GDPR", *Misc*, 94, November/December 2017, 74-82.

[2] Denis VIOLE, "L'évolution de la fonction CIL vers la fonction DPO", *Misc*, 90, Mars/Avril 2017, 72-77.

[3] 2016. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (Texte that present the interest for the l'EEE) [onligne]. 4 may 2016. S.l.: s.n. [Consult the 29 october 2017]. Available at the address http://data.europa.eu/eli/reg/2016/679/oj/fra

[4] Dataviz sur le règlement européen sur la protection des données. In: [online]. [Consul the 13 november 2017]. Available at the address https://www.cnil.fr/fr/reglement-europeen-protection-donnees/dataviz#

[5] Devenir délégué à la protection des données | CNIL. In: [online]. [Consult the 15 november 2017]. Available at the address https://www.cnil.fr/fr/devenir-delegue-la-protection-des-donnees

[6] GDPR.expert, l'outil d'analyse du nouveau règlement européen, développé par le cabinet d'avocats Ulys. In: GDPR.expert [online]. [Consult the 2 novembre 2017]. Available at the address http://www.gdpr-expert.eu/

[7] Lignes directrices | CNIL. In: [online]. [Consult the 15 novembre 2017]. Available at the address https://www.cnil.fr/fr/reglement-europeen/lignes-directrices

[8] Règlement européen: encore un an pour se préparer | CNIL. In: [online]. [Consult the 15 november 2018]. Available at the address https://www.cnil.fr/fr/reglement-europeen-encore-un-pour-se-preparer

[9] RGPD: un logiciel pour réaliser son analyse d'impact sur la protection des données (PIA) | CNIL. In: [online]. [Consult the 15 november 2017]. Available at the address https://www.cnil.fr/fr/rgpd-un-logiciel-pour-realiser-son-analyse-dimpact-sur-la-protection-des-donnees-pia

[10] VOLLMER, Nicholas, 2017. Table of contents EU General Data Protection Regulation (EU-GDPR). In: [online]. 16 décembre 2017. [Consult the 20 december 2017]. Available at the address http://www.privacy-regulation.eu/en/

[11] Six-Step Guide to GDPR Preparation, March 17, 2017. Available at the address : https://onetrust.com/cnil-six-step-guide-gdpr-preparation/

[12] CNIL, Règlement européen : se préparer en 6 étapes. Available at the address : https://www.cnil.fr/fr/principes-cles/reglement-europeen-se-preparer-en-6-etapes

[13] CNIL, La protection des données dans le monde. Available at the address https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde