How can companies comply with 2018 GDPR regulation while earning benefits?[1, 2]

Etienne Plassard

ABSTRACT

As a reaction to the General Data Protection Regulation (GDPR) implemented on May 25th of 2018, companies seek compliance and better data privacy management. Besides, lots of them are still struggling with processes implementation. This paper aims at offering concrete solutions to start and improve their overall GDPR compliance while earning benefits and saving costs. This study will answer the following research questions: how to deal with data-privacy contract management, how to manage data efficiently, and how to mitigate risks related to data breaches. The research method used to evaluate the different solutions is the additive weighting technique based on a compensation model. We will find that the four best alternatives must be combined to ensure significant GDPR compliancy and benefits. Thus, adopting a performant contract management system and having a strong breach identification is necessary, as well as using the Agile methodology to implement change.

Keywords: Cash Flows, Data, Protection, GDPR, Compliance, Risk Mitigation, Storage, Breaches, Cybersecurity, CMS, Anonymization

INTRODUCTION

Do you think it is normal that today, only one in five companies surveyed believe they are GDPR compliant? This famous agreement on data protection implemented since May 25th of 2018 reveals not to be respected by a wide majority of US and European companies.[3]

The problem is complex for many reasons: "GDPR's scope is far more comprehensive and wide-reaching, meaning businesses will need to amend their data protection policies accordingly", says

[1] Editor's note: Student papers are authored by graduate or undergraduate students based on coursework at accredited universities or training programs. This paper was prepared for the course "International Contract Management" facilitated by Dr Paul D. Giammalvo of PT Mitratata Citragraha, Jakarta, Indonesia as an Adjunct Professor under contract to SKEMA Business School for the program Master of Science in Project and Programme Management and Business Development. http://www.skema.edu/programmes/masters-of-science. For more information on this global program (Lille and Paris in France; Belo Horizonte in Brazil), contact Dr Paul Gardiner, Global Programme Director, at paul.gardiner@skema.edu.

[2] How to cite this paper: Plassard, E. (2019). How can companies comply with 2018 GDPR regulation while earning benefits? *PM World Journal*, Vol. VIII, Issue VII, August.

[3] *Edward Gately, 80 Percent of Companies Still Not GDPR-Compliant (*2018, July*)*. Retrieved from: https://www.channelpartnersonline.com/2018/07/13/80-percent-of-companies-still-not-gdpr-compliant/

a Virtual College study.[4] There are way more clauses to comply with than the previous 1995 DPA and the volume of data concerned is tremendous for big corporations. It represents also a deep shift in people ways of working, as well as huge IT organizational and process changes. In parallel, data privacy stakes are rising: the Ponemone Institute found increasing data breaches in frequency (33% in 2013 and 43% in 2014)[5] while Verizon confirmed 53,000 incidents and 2,216 confirmed data breaches in 2018[6]. On top of that, the legal part remains the major concern of GDPR, however, it is also a question of freedom, respect, and dignity of the people[7].

One can realize all these major changes cannot be implemented once and for all, even more on a short-time period. In this study, we will develop actions and processes companies can use to tend to full GDPR compliancy while earning benefits at the same time. It is something very progressive companies must work on because it targets not only data management but also change and risk management. On top of that, this very wide project must be seen as a long-term process to put in parallel with a global better data privacy management. According to Daniel Mintz, “All businesses housing large volumes of data are faced with a dilemma: figuring out which data to keep and ensuring that data that is kept is secure”.[8] Indeed, these structures are at the edge of transformation and integration solutions that help their clients managing their databases. We will narrow the study to EU and US companies that can afford the solutions furtherly approached, starting from medium-sized companies up to corporations.

In this study, we will enlighten three major issues companies must face and their related solutions. First, data-related contract management becomes a nightmare when it comes to checking on every clause. Identifying the data nature and stakeholders concerned is the first step to a long process, not to mention US and EU differences and opening clauses that “permit a Member State to modify the provisions of the Article” for a “more restrictive application of the GDPR obligation via local legislation.”[9] In parallel, companies must tackle data issues such as increasing data volume and

[4] *What are the main differences between the GDPR and the Data Protection Act?* Conducted by Virtual College (2018, January). Retrieved from: https://www.virtual-college.co.uk/news/virtual-college/2018/01/the-differences-between-gdpr-and-data-protection

[5] *Is Your Company Ready for a Big Data Breach?* Conducted by Ponemon Institute (2013, April) Retrieved from http://www.experian.com/assets/data-breach/brochures/2014-ponemon-2nd-annual-preparedness.pdf

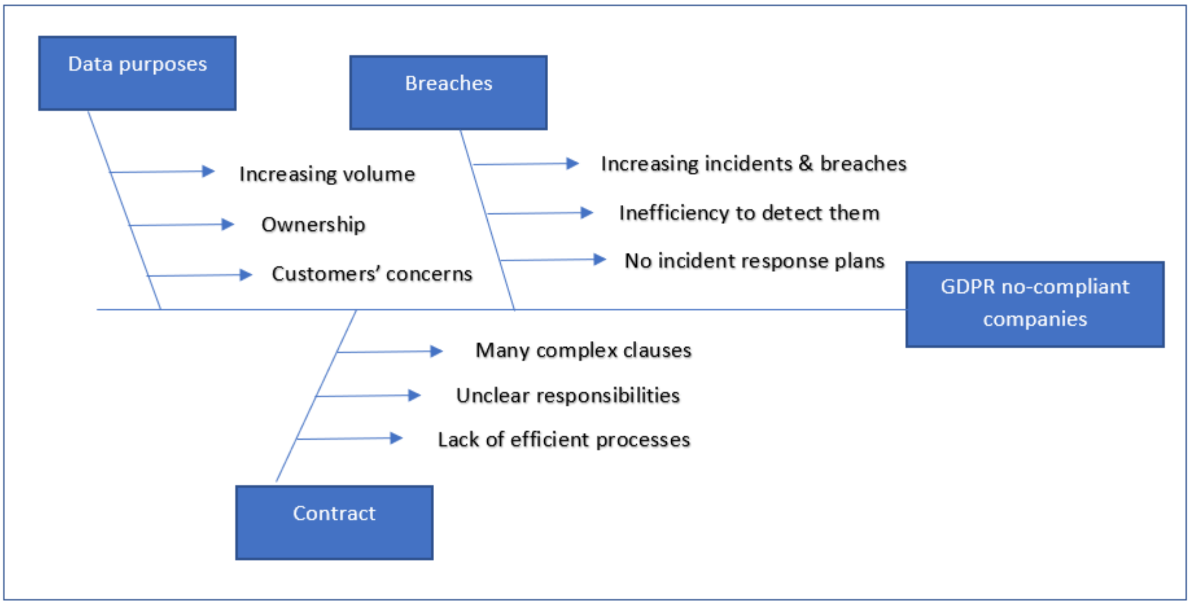
[6] *2018 Data Breach Investigations Report, 11th edition*, conducted by Verizon (2018). Retrieved from: http://www.documentwereld.nl/files/2018/Verizon-DBIR_2018-Main_report.pdf

[7] Laxmi Sharma, GDPR: After 25th May, *What Medium And Long-Term Actions?* (2018, June). Retrieved from: https://www.smartdatacollective.com/gdpr-25th-what-medium-long-term-actions/

[8] Daniel Mintz, *The Road to Becoming GDPR Compliant Leads to Log Term Success*, (2018, October). Retrieved from: http://www.dataversity.net/road-becoming-gdpr-compliant-leads-long-term-success/

[9] John Tomaszewski, *“Opening Clauses” in the GDPR – It Might Not Be As Easy As We Thought* (2017, July). Retrieved from*:* *https*://www.globalprivacywatch.com/2017/07/opening-clauses-and-the-gdpr-it-might-not-be-as-easy-as-we-thought/

relevancy. For example, "you may need to appoint a data protection officer (DPO), depending on the types of processing your company conducts"[10], to tackle daily and long-term data privacy purposes. Launching data minimization and anonymization processes should reduce sensitive data ownership because according to Recital 26 of GDPR, "The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable"[11]. Thus, the ability to use this kind of data can help companies improve their customers' experience, or simply be a new source of profit.[12]
The last big issue is about incident and breaches. How to deal with them? It starts with a complete protection and prevention program: breach identification is necessary, as well as a permanent cybersecurity control through bounty programs for example. Because risks cannot be all avoided, companies must have solid and very-well processed incident response plans to anticipate costs, resources and decisions related to every possible breach situation[13].


Data purposes
Increasing volume
Ownership
Customers' concerns
Breaches
Increasing incidents & breaches
Inefficiency to detect them
No incident response plans
GDPR no-compliant companies
Many complex clauses
Unclear responsibilities
Lack of efficient processes
Contract

Cause and effect diagram[14]

[10] Lei Shen, Rebecca Eisner, *Updating Your Vendor Agreements to Comply With GDPR* (2017, March). Retrieved from: https://iapp.org/news/a/updating-your-vendor-agreements-to-comply-with-gdpr/

[11] Recital 26 EU GPDR, (2018, September). Retrieved from: http://www.privacy-regulation.eu/en/recital-26-GDPR.htm

[12] *How To Monetize Your Data?* produced by Lotame (2018, February). Retrieved from: https://www.lotame.com/how-to-monetize-your-data/

[13] Elizabeth Kemery Sipes, Bryan Cave, Joshua James, *Current data security issues for financial services firms* (n.d). Retrieved from: https://www-emeraldinsight-com.ezp.skema.edu/doi/full/10.1108/JOIC-07-2016-0034

[14] By the author

Project management shall be used by companies that want to be GDPR compliant. In this case, Agile methodology is the most appropriate because DPOs and team members need short-term strings and continuous feedback to progress in this long-term project[15].

The development of this article will answer to the following problematic: "How can companies increase their cash flows and savings through GDPR compliance processes?

The purpose of this essay will be to demonstrate that companies have relevant tools to improve their data management while performing a profitable GDPR compliancy plan.

To do this, we will first discuss how to deal with GDPR clauses and use tools to better manage data-related contracts. Then, we will see how to manage data and its ethical related issues. Finally, we will tackle breaches issues and describe how to mitigate the associated risks.

METHODOLOGY

STEP 1: Problem recognition, definition, and evaluation

As described in the first part of the paper, the aim is here to find the best methods to improve companies' GDPR compliancy while implementing profitable processes. To do so, a detailed analysis of the three major issues of data and contract management is needed. The objective here is to consider the different alternatives that can be practically applied to solve this very big GDPR compliancy issue.

STEP 2: Development of feasible alternatives

Before listing all the solutions, there are some prerequisites for the company to fulfill to be able to implement processes. First, the company needs to hire or name a Data Protection Officer (DPO) responsible for technical aspects[16]: he will have to know everything about GDPR regulation and opening clauses.

Solutions to deal with technical contract aspects:

- **Create a unique storage place** so that it is easier, safer and quicker to access to sensitive data. Companies can create different access levels for employees for a safer data management. An encrypted cloud service is perfect to store all contracts[17].

[15] Agile GDPR Compliance Management: An End-To-End Process leveraging Artificial Intelligence. (2018, July). Retrieved from https://blog.confidentgovernance.com/2018/07/12/agile-gdpr-compliance-management-an-end-to-end-process-leveraging-artificial-intelligence/

[16] Do you need to hire a DPO? Produced by Talentarc. (2018, May 14). Retrieved from: https://www.talentarc.com/do-you-need-to-hire-a-dpo/

[17] Ivey, V. 5 Tips to Keep Your Data Secure on the Cloud. (2013, December 16). Retrieved from: https://www.cio.com/article/2380182/cloud-security/5-tips-to-keep-your-data-secure-on-the-cloud.html

- **Authoring Solutions:** Using a software with contract authoring capabilities allows to manage day-to-day operations, especially from a data controller position. Contract automation may solve a substantial number of problems of traditional contracting. Different business units will be driven by the same motivation: create, send and execute contracts quicker.

- **A Contract Event Tracking system:** it refers to savings on administrative and operating costs and thus accelerates revenues. The implemented reminders will warn you so that you never miss renewals or opportunities to renegotiate with vendors.

Much available software on the market run and gather these three solutions, such as Precisely, Conga, Gatekeeper, or Icertis, so we will study a general solution called "**A performant Contract Management Solution**".

Solutions to deal with data and ethical related problems

- **Data minimization:** a very powerful measure to "retain the least amount of personal information in order for an organization to function."[18]. The objective here is people privacy protection. In that way, less information needs protection and storage and avoidable data breaches are prevented. It requires organizations to identify where to collect information and why. Companies may also have to make decisions, for example, if specific kind of data is necessary from a business perspective.

- **Data pseudonymization:** De-identification must be considered as a general concept that ranges from simple pseudonymization to full anonymization. Pseudonymization refers to enhancing privacy by replacing most identifying fields within a data record by pseudonyms, meaning one or more artificial identifier.[19]. "Pseudonymized data remains "personal data" and is therefore subject to the requirements of the GDPR."[20] As concerns pseudonymized data, the full range of mandated disclosures applies.

- **Data full anonymization:** contrary to pseudonymized data, because anonymized data is no longer considered personal data, none of the GDPR obligations apply to fully anonymized data that meets European requirements[21].

[18] Gatekeeper. (n.d.). Gatekeeper Contract Management. Retrieved from https://www.gatekeeperhq.com/contract-management-lp?utm_source=capterra&utm_medium=cpc&utm_term=contract-management&utm_content=v1&utm_campaign=capterra-contract-mgmt&capchannel=GetApp

[20] Current data security issues for financial services firms, Produced by Emerald Group Publishing Limited. (2013, December 16). Retrieved from https://www-emeraldinsight-com.ezp.skema.edu/doi/full/10.1108/JOIC-07-2016-0034

[21] Data masking: anonymization or pseudonymization? GDPR.Report. (2017, September 28). Retrieved from: https://gdpr.report/news/2017/09/28/data-masking-anonymization-pseudonymization/

- **The right to erase & the right to be forgotten:** principles used to solve ethical problems. They tell about how to draw the line between security, privacy, and innovation. In many cases, what is at stake is striking the perfect balance between privacy, innovation and security[22].

Solutions to deal with breaches

- **Breach identification and prevention:** "Data breach detection technologies are not often deployed. Despite the increase in data breaches, slightly less than half of respondents (48 percent) say their organizations made an investment in technologies to detect and respond to a data breach".[23] So first, companies should first be prepared with efficient and reliable solutions such as anti-viruses, intrusion prevention systems or MDM to detect and prevent as many breaches as possible.

- **Bounty programs:** Companies can use forums to communicate with hackers and pay them to identify and report vulnerabilities. "Organizations proactively encourage the public to report security vulnerabilities by paying well-meaning hackers (usually called "white hat hackers" or "independent researchers") to report problems.[24]

- **Incidence response plan:** The aim here is not to be able to predict any kind of breach. It fundamentally states who is responsible for security incident investigations, "what resources that person has at his or her disposal (inside and outside of the organization), and when a situation should be elevated to involve others within the organization".[25]

- **Launch a long-term Agile GDPR compliance process:** a classical step-by-step procedure to increase the percentage of compliance, comprising iterative processes, as well as short loops feedback system. It also requires regular check-ups and long-term objectives[26].

[22] Art. 17 GDPR? Right to erasure ('right to be forgotten?), General Data Protection Regulation (GDPR). (n.d.). Retrieved from: https://gdpr-info.eu/art-17-gdpr/

[23] Is Your Company Ready for a Big Data Breach? Sponsored by Experian® Data Breach Resolution, conducted by Ponemon Institute, (2013, April) http://www.experian.com/assets/data-breach/brochures/2014-ponemon-2nd-annual-preparedness.pdf

[24] Current data security issues for financial services firms, Emerald Group Publishing Limited. (2016) Retrieved from: https://www-emeraldinsight-com.ezp.skema.edu/doi/full/10.1108/JOIC-07-2016-0034

[25] Current data security issues for financial services firms, Emerald Group Publishing Limited. (2016) Retrieved from: https://www-emeraldinsight-com.ezp.skema.edu/doi/full/10.1108/JOIC-07-2016-0034

[26] Agile GDPR Compliance Management: An End-To-End Process leveraging Artificial Intelligence. (2018, July 12). Retrieved from https://blog.confidentgovernance.com/2018/07/12/agile-gdpr-compliance-management-an-end-to-end-process-leveraging-artificial-intelligence/

We have been here through the feasible alternative solutions, and we will now deal with the attributes that we are going to measure and evaluate each one of them.

- **Increase data cybersecurity & people privacy:** what is here at stake is to protect sensitive data to preserve people privacy, and thus prevent breaches and improve customer loyalty. Organizations must respond to increasing customer awareness and pressure on their data security[27].

- **Increase cash flows and savings:** as the main objective of a company is profitable, it definitively needs to boost its cash flows and save money. GDPR compliancy can be a real commercial opportunity, as companies can communicate their competitive strengths to their customers. "Not only do [companies] respect the regulation in the eyes of my users or customers, but [they] propose to them, by being transparent, to take advantage of them to improve the service".[28]

- **Mitigate fine risks:** the aim here is to reduce the risk of being GDPR non-compliant because the company can be exposed "up to €20 million, or 4% of the worldwide annual revenue of the prior financial year".[29]

- **Reduce legal procedures:** companies cannot be subject to a tremendous number of costly and time-consuming legal procedures, not to consider the devastating impact on their brand image. If data is better managed, there is a lower risk of breaches and thus lower number of legal procedures.[30]

- **Time-Saving:** in every business, time equals money. It is necessary for companies to save time in any process by having a clear agenda and detailed processes. Short-term procedures are easier to implement and will necessitate fewer efforts and costs. Time-saving can be done through organizational measures such as planning and structuring tasks.[31]

- **Flexibility:** the solutions we want to analyze must be as easy to handle as possible, meaning we will determine to what extent the project that can undergo changes on

[27] Cybersecurity and data privacy: what are you overlooking? (2018, July 13). Retrieved from https://www.itproportal.com/features/cyber-security-and-data-privacy-what-are-you-over-looking/

[28] Laxmi Sharma, GDPR: After 25th May, *What Medium And Long-Term Actions?* (2018, June). Retrieved from: https://www.smartdatacollective.com/gdpr-25th-what-medium-long-term-actions/

[29] Fines and Penalties, produced by GDPR EU.org. (n.d.). Retrieved from: https://www.gdpreu.org/compliance/fines-and-penalties/

[30] 15 ways to prevent data security breaches, produced by Big Data Made Simple. (2018, October 5). Retrieved from: https://bigdata-madesimple.com/15-ways-to-prevent-data-security-breaches/

[31] Time-Saving Methods to Prioritise Your GDPR Compliance. Produced by Nymity (2018, August 10). Retrieved from: http://blog.nymity.com/blog/time-saving-methods-to-prioritise-your-gdpr-compliance

processes or deliveries throughout its establishment. On the contrary, there are some GDPR principles for which there is no tolerance.[32]

- **Monitoring and control:** it is crucial that processes are well-managed and procedures are properly applied so that the solution implementation process goes as smoothly as possible. The Data Protection Officer (DPO) plays a cornerstone role in the process.[33]

- **Increase customer loyalty:** the customer point of view is determinant for every company because it will widely influence future sales in the long term. Having a strong customer loyalty makes the business economically sustainable.[34]

- **Effectiveness:** this attribute will help us evaluate the global impact of the solution short-term and long-term speaking compared to the initial investment. It can be based on time, cost, benefits or brand influence.[35]

- **Specific:** the project goal must be well-defined and clear to every stakeholder that has a basic implication in the project.[36]

- **Measurable:** it refers to the metrics used to measure the progress and the benefits of the project when completion is achieved.[35]

- **Achievable:** it refers to the agreement on the definition of completion with stakeholders.[35]

- **Realistic:** the objective of the solution is reachable with given resources, time and knowledge.[35]

- **Time-based:** the whole project necessitates reasonable but not too much time to achieve the expected goals. Tasks and objectives are time-based.[35]

[32] France: Pragmatism and Flexibility for the GDPR Implementation | Password Protected. (2018, February 20). Retrieved from: https://www.passwordprotectedlaw.com/2018/02/france-pragmatism-and-flexibility-for-the-gdpr-implementation/

[33] GDPR Compliance Monitoring. (2018, June 12). Retrieved from: https://www2.deloitte.com/mt/en/pages/risk/articles/mt-risk-article-gdpr-monitoring.html

[34] GDPR and the Road to Increased Customer Loyalty and Trust - Security Thinking Cap. (2018, June 12). Retrieved from: https://securitythinkingcap.com/gdpr-increase-customer-loyalty-trust/

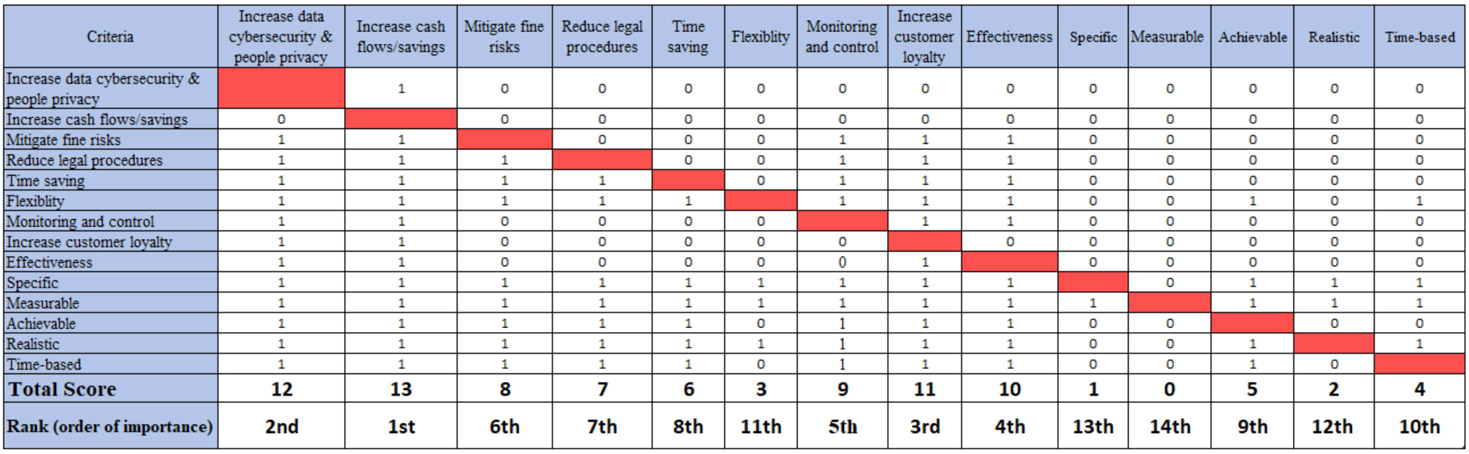
[35] GDPR Best Practices Implementation Guide. (n.d.). Retrieved from https://www.infosecurityeurope.com/__novadocuments/355669?v=636289786574700000

[36] Corporate SMART Goal, *SMART Goal*, (n.d.). Retrieved from: https://corporatefinanceinstitute.com/resources/knowledge/other/smart-goal/

STEP 3: Development of feasible alternatives

We will here rank the possible solutions developed above using a non-compensatory model and disjunctive reasoning. We will thus determine which attributes are the most important. We will give a score of 1 to the best options and 0 for the worst ones.[37]

We will use a simple comparison method to rank these criteria from the 1st to the 14th.



Criteria	Increase data cybersecurity & people privacy	Increase cash flows/savings	Mitigate fine risks	Reduce legal procedures	Time saving	Flexiblity	Monitoring and control	Increase customer loyalty	Effectiveness	Specific	Measurable	Achievable	Realistic	Time-based
Increase data cybersecurity & people privacy		1	0	0	0	0	0	0	0	0	0	0	0	0
Increase cash flows/savings	0		0	0	0	0	0	0	0	0	0	0	0	0
Mitigate fine risks	1	1		0	0	0	1	1	1	0	0	0	0	0
Reduce legal procedures	1	1	1		0	0	1	1	1	0	0	0	0	0
Time saving	1	1	1	1		0	1	1	1	0	0	0	0	0
Flexiblity	1	1	1	1	1		1	1	1	0	0	1	0	1
Monitoring and control	1	1	0	0	0	0		1	1	0	0	0	0	0
Increase customer loyalty	1	1	0	0	0	0	0		0	0	0	0	0	0
Effectiveness	1	1	0	0	0	0	0	1		0	0	0	0	0
Specific	1	1	1	1	1	1	1	1	1		0	1	1	1
Measurable	1	1	1	1	1	1	1	1	1	1		1	1	1
Achievable	1	1	1	1	1	0	1	1	1	0	0		0	0
Realistic	1	1	1	1	1	1	1	1	1	0	0	1		1
Time-based	1	1	1	1	1	0	1	1	1	0	0	1	0	
Total Score	**12**	**13**	**8**	**7**	**6**	**3**	**9**	**11**	**10**	**1**	**0**	**5**	**2**	**4**
Rank (order of importance)	**2nd**	**1st**	**6th**	**7th**	**8th**	**11th**	**5th**	**3rd**	**4th**	**13th**	**14th**	**9th**	**12th**	**10th**

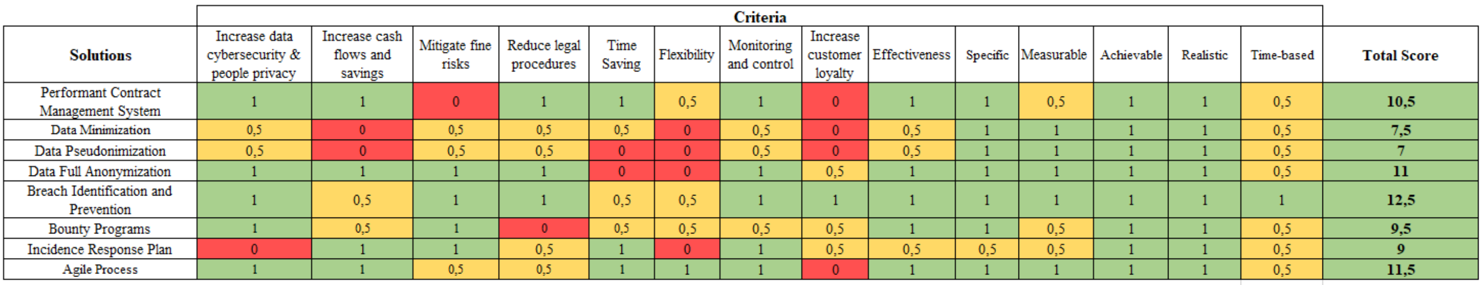
Table 2: Non-compensatory Model using Disjunctive Reasoning[38]

As a consequence, the most important criteria are cash flows and savings, followed by cybersecurity and people privacy purposes. On the contrary, Flexibility and Time-Saving appear not to be priorities, not to say they are not irrelevant though.

STEP 4: Selection of criteria

The final step should be to select the top alternatives that will appear on the following chart. We will use a compensatory model, using a non-dimensional scaling technique. Each alternative solution will be evaluated from "excellent" to "worse".

Let's now assume this:



	Criteria														
Solutions	Increase data cybersecurity & people privacy	Increase cash flows and savings	Mitigate fine risks	Reduce legal procedures	Time Saving	Flexibility	Monitoring and control	Increase customer loyalty	Effectiveness	Specific	Measurable	Achievable	Realistic	Time-based	**Total Score**
Performant Contract Management System	1	1	0	1	1	0,5	1	0	1	1	0,5	1	1	0,5	**10,5**
Data Minimization	0,5	0	0,5	0,5	0,5	0	0,5	0	0,5	1	1	1	1	0,5	**7,5**
Data Pseudonimization	0,5	0	0,5	0,5	0	0	0,5	0	0,5	1	1	1	1	0,5	**7**
Data Full Anonymization	1	1	1	1	0	0	1	0,5	1	1	1	1	1	0,5	**11**
Breach Identification and Prevention	1	0,5	1	1	0,5	0,5	1	1	1	1	1	1	1	1	**12,5**
Bounty Programs	1	0,5	1	0	0,5	0,5	0,5	0,5	1	1	0,5	1	1	0,5	**9,5**
Incidence Response Plan	0	1	1	0,5	1	0	1	0,5	0,5	0,5	0,5	1	1	0,5	**9**
Agile Process	1	1	0,5	0,5	1	1	1	0	1	1	1	1	1	0,5	**11,5**

[37] Planning Planet (Nov-2015) – *Guild of Project Controls Compendium and Reference (CaR) – 10.3.3.7 Multi-Attribute Decision Making*. Retrieved from: http://www.planningplanet.com/guild/gpccar/managing-change-the-owners-perspective

[38] By Author

Excellent	Fair	Bad
1	0,5	0

Table 3: Analysis of the alternative solutions based on a Compensation Model[39]

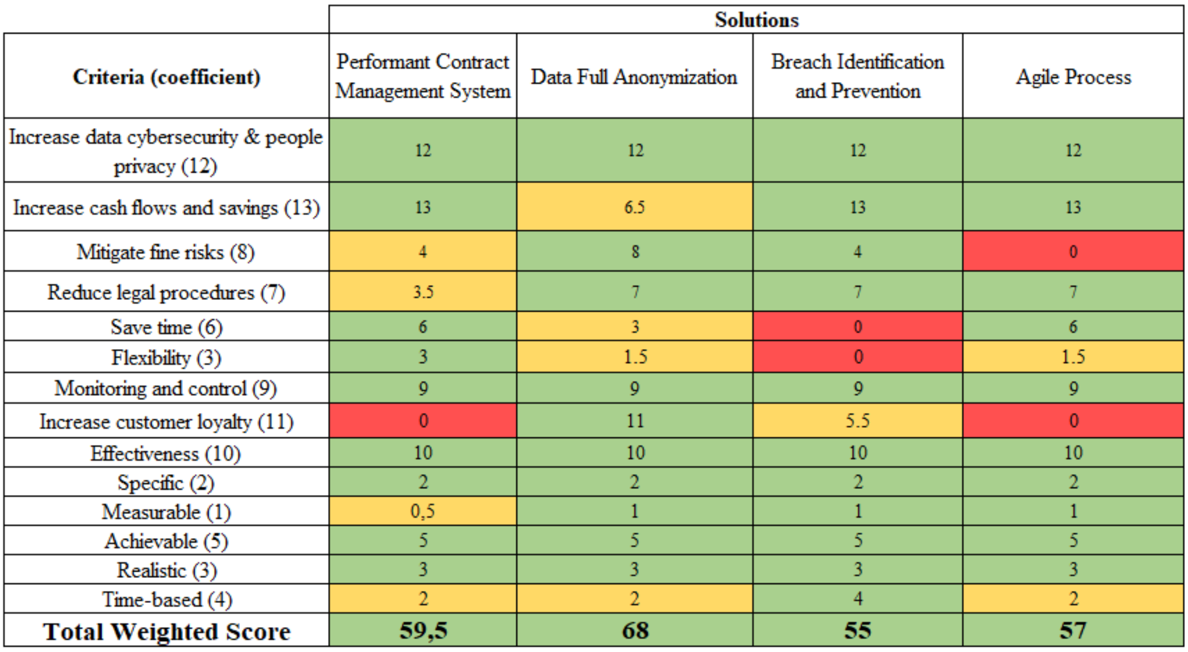
Feasible solutions rank from 7 to 12,5. We will set a 10-score acceptable limit: any alternative under this score will not be analyzed. Nevertheless, we can identify two alternatives that are relevant to implement but not critical: bounty programs and incidence response plan.

Finally, 4 solutions will be tackled:

- Breach Identification
- Data Full Anonymization
- Agile long-term process
- A performant Contract Management system

STEP 5: Analysis and comparison of the alternatives

The method leads us to evaluate our project using an additive weighting technique, still based on a compensation model. It will allow us to compare the four best alternatives. Criteria will be weighted according to their relative rank, from coefficient 1 for “Flexibility” to coefficient 14 for “Increasing Cash Flows and Savings”.



	Solutions			
Criteria (coefficient)	Performant Contract Management System	Data Full Anonymization	Breach Identification and Prevention	Agile Process
Increase data cybersecurity & people privacy (12)	12	12	12	12
Increase cash flows and savings (13)	13	6.5	13	13
Mitigate fine risks (8)	4	8	4	0
Reduce legal procedures (7)	3.5	7	7	7
Save time (6)	6	3	0	6
Flexibility (3)	3	1.5	0	1.5
Monitoring and control (9)	9	9	9	9
Increase customer loyalty (11)	0	11	5.5	0
Effectiveness (10)	10	10	10	10
Specific (2)	2	2	2	2
Measurable (1)	0,5	1	1	1
Achievable (5)	5	5	5	5
Realistic (3)	3	3	3	3
Time-based (4)	2	2	4	2
Total Weighted Score	**59,5**	**68**	**55**	**57**

Table 3: Analysis of the alternative solutions based on a Compensation Model[40]

[39] By Author
[40] By Author

Considering all, Data full anonymization appears to be the most important processes because it allows the company to earn huge revenues or a nice brand image. Nevertheless, companies must absolutely run a performant Contract Management System and an Agile long-term process to ensure an acceptable level of GDPR compliancy. Breach Identification and prevention will be priority number 4.

STEP 6: Selection of the preferred alternatives

In this step, we will further define and analyze the four preferred alternatives to understand how they can be implemented and what conditions are required for them to be applied.

Data Full anonymization: As said below, pseudonymized data is still considered as personal data, and it is, therefore, subject to the GDPR requirements. In the case of full anonymization, companies benefit from information no longer considered as personal data. Thus, none of the GDPR obligations apply to fully anonymized data that meets European requirements[41]. In this case, companies have two main choices. On one hand, some may keep anonymized data to have a competitive advantage. On top of that, they can communicate on the fact they protect their customer privacy in order to reinforce customer trust and loyalty, with a boosting effect on revenues eventually.[42] On the other hand, some companies may decide to sell fully anonymized data to third parties such as advertisers to make huge benefits. For instance, Facebook collects all the content you provide when using their services, such as locations, photos, videos and messages. The company knows your friends and all your activities, so it can sell this information to advertisers. "Facebook trackers are just about everywhere on the Internet. But because most of Facebook's 1.49 billion users routinely access the service through an app, the ads cannot be hidden using one of the many blocker tools."[43] It allowed Facebook to earn more than 33 billion dollars in sales advertising in 2018.[44]

Adopting a performant Contract Management System: a powerful solution that will solve a substantial number of problems in traditional contracting and data storage. First, having a unique storage place that makes easier, safer and quicker to access to sensitive data. Companies can create different access levels for employees for a safer data management. As a result, all contracts are stored in a very secure place, that widely lowers breaches incidents. An encrypted cloud service is a very practical solution to store all contracts, but even this cannot protect any user from leaks.

[41] Data masking: anonymization or pseudonymization? GDPR.Report. (2017, September 28). Retrieved from: https://gdpr.report/news/2017/09/28/data-masking-anonymization-pseudonymization/

[42] GDPR: After 25th May, What Medium And Long-Term Actions? (2018, June 8). Retrieved from: https://www.smartdatacollective.com/gdpr-25th-what-medium-long-term-actions/

[43] The price of free: how Apple, Facebook, Microsoft and Google sell you to advertisers. (2015, October 1). Retrieved from: https://www.pcworld.com/article/2986988/privacy/the-price-of-free-how-apple-facebook-microsoft-and-google-sell-you-to-advertisers.html

[44] U.S. Facebook advertising revenue 2018, produced by Statistic. (2018). Retrieved from: https://www.statista.com/statistics/544001/facebooks-advertising-revenue-worldwide-usa/

Nevertheless, it remains blurred about which law of which country regulates data privacy content[45]. Moreover, using a solution with contract authoring capabilities allows companies to manage day-to-day operations, especially from a data controller position. Different business units will be driven by the same motivation: create, send and execute contracts quicker. These solutions will provide a complete overview of contract monitoring and control to perform end-to-end contract management.[46] It allows also to reduce conflicts between parties and gets you legally covered (Information Security Management System compliant with ISO 27001 & ISO 9001 norms). Finally, having a Contract Event Tracking feature in the solution provides savings on administrative and operating costs and thus accelerates revenues. The implemented reminders will warn you so that you never miss renewals or opportunities to renegotiate with vendors. After a quick overview, much available software on the market run and gather these three solutions, such as Precisely, Conga, Gatekeeper, or Icertis.

The Agile Methodology is particularly adapted to comply with GDPR regulation. The aim is to develop long-term incremental and automated processes to improve the percentage of compliance. Developing incrementally means getting the basic product working as fast as possible and then refine and improve the product until it satisfies the regulations. A basic principle of Agile is to set time, cost and quality: only the delivered features can evolve over time. The company must focus on individuals and interactions rather than processes and tools. In the same way, responding to change is more important than following the plan. The team roles and responsibilities must be clearly defined. Through milestones, attributes and exceptions tracking, the Agile methodology provides remediation actions to improve GDPR compliance. Moreover, using MoSCoW prioritization principle allows determining the “Must have” referring to the minimum usable subset and the “Should have” that represents important but not vital features[47].

The Agile CRM is committed to complying with the GDPR act, in addition to helping customers stay compliant with the said regulations. It has defined and implemented the requisite security requirements, while continuously keeping track of changes in the GDPR implementation policy. Thus, it provides updates on GDPR-readiness status regarding categories of processing activities, information regarding data transfers, and general security measures.[48] On the long-term, the whole process brings risk avoidance, reputational protection, effective data governance as well as benefits from organizational change and tangible savings opportunities identification.[49]

[45] Ivey, V. 5 Tips to Keep Your Data Secure on the Cloud. (2013, December 16). Retrieved from: https://www.cio.com/article/2380182/cloud-security/5-tips-to-keep-your-data-secure-on-the-cloud.html

[46] GDPR & Contract Management? 5 Must-Have Features. (2018, September 7). Retrieved from: https://precisely.se/2018/04/18/gdpr-contract-management/

[47] APMP International. (n.d.). *Agile Project Management*. Retrieved from https://www.trainingbytesize.com/?lang=fr

[48] Agile CRM - GDPR Compliance. (n.d.). Retrieved from: https://www.agilecrm.com/gdpr-compliance

[49] GDPR – Threat or Opportunity? – We are Lean and Agile. (n.d.). Retrieved from: https://weareleanandagile.com/uncategorized/gdpr-threat-or-opportunity/

Breach Identification and Prevention: A data breach occurs when a cybercriminal succeeds to extract sensitive information "by physically accessing a computer or network to steal data or by bypassing network security remotely".[50] Preventing these breaches consists in deploying the most complete possible arsenal that detects breaches and protects the company's data from outside attacks. It must be composed of efficient anti-viruses, intrusion prevention systems or MDM to detect and avoid as many intrusions as possible. A Mobile Device Management (MDM) is a software that allows IT administration to control and secure policies on smartphones, tablets and other devices. In that way, companies "optimize the functionality and security of mobile devices within the enterprise while simultaneously protecting the corporate network"[51]. A good protection method is to make sure the company has "malware detection software running on both your servers (hosted or not) and workstations and ensure that your firewalls are up and secure"[52]. Breach prevention also targets employees because they are the ones who gather customer information and face phishing emails, worms and other kinds of malware. Having employees unaware that they handle sensitive information and can easily leak data is a major weakness[53]. Employees must be trained through awareness programs to assimilate appropriate conducts concerning data management.

STEP 7: Performance Monitoring and post-evaluation of results

After having fully analyzed these four solutions, we must review their relative importance established in step 5. At first, it has been found that Data Full Anonymization was the most important criteria. Nevertheless, it turns out GDPR compliancy cornerstone is to centralize contracts and data and standardize your processes, that means using a performant contract management system. In that way, the next step must be to launch a long-term compliance process, for example following the Agile methodology to show the European Union it makes efforts to comply with European regulations. As a result, doing these two first steps will mitigate both legal procedures and fine risks. Then, for the company to be profitable, it must compensate expenses related to breaches prevention with all benefits coming from data sales or improved brand image. In a few words, even if the main objective of companies is to be profitable, they must think first about long-term vision. They must rather take into consideration sustainability and competitive advantages, and thus, if not already done, adopt first a solid Performant Contract Management System, and launch their Agile compliancy process.

[50] Data Breaches 101: How They Happen, What Gets Stolen, and Where It All Goes - Security News - Trend Micro USA. (n.d.). Retrieved from https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/data-breach-101

[51] What is mobile device management (MDM)? - Definition from WhatIs.com. (n.d.). Retrieved from: https://searchmobilecomputing.techtarget.com/definition/mobile-device-management

[52] Marks, G. (2014, June 23). 7 Ways To Protect Yourself Against A Data Breach. Retrieved from: https://www.forbes.com/sites/quickerbettertech/2013/12/31/7-ways-to-protect-yourself-against-a-data-breach/#

[53] Is Your Company Ready for a Big Data Breach? Sponsored by Experian® Data Breach Resolution, conducted by Ponemon Institute (2013, April). Retrieved from: http://www.experian.com/assets/data-breach/brochures/2014-ponemon-2nd-annual-preparedness.pdf

CONCLUSION

When it comes to GDPR compliancy, one must understand companies have to implement simultaneously several processes to allow significant progress. The combination of all the solutions introduced below will permit companies to be profitable on a long-term basis. Firstly, companies must have a performant contract and data management system to gain security and efficiency purposes. Moreover, companies must protect themselves from other potential breaches through training programs and efficient tools. These expenses can be compensated whether by revenues coming from additional sales due to a strong customer loyalty or by advertising revenues. Finally, the overall GDPR compliancy process should be monitored through a continuous step-by-step Agile methodology in order to improve the percentage of compliance. Applying these solutions should mitigate legal risks and increase revenues. Of course, all benefits cannot be concretely measured especially for the company's brand image. Thus, the combination of these 4 solutions is necessary for the long-term as it provides security follow-up and competitive advantages.

BIBLIOGRAPHY:

1. *Edward Gately, 80 Percent of Companies Still Not GDPR-Compliant*, (2018, July 13). Retrieved from: https://www.channelpartnersonline.com/2018/07/13/80-percent-of-companies-still-not-gdpr-compliant/

2. *What are the main differences between GDPR and the Data Protection Act?* Conducted by Virtual College, (2018, 2nd of January). Retrieved from: https://www.virtual-college.co.uk/news/virtual-college/2018/01/the-differences-between-gdpr-and-data-protection

3. *Is Your Company Ready for a Big Data Breach?* Conducted by Ponemon Institute, (2013, April). Retrieved from: http://www.experian.com/assets/data-breach/brochures/2014-ponemon-2nd-annual-preparedness.pdf

4. *2018 Data Breach Investigations Report, 11th edition*, conducted by Verizon, (2018). Retrieved from: http://www.documentwereld.nl/files/2018/Verizon-DBIR_2018-Main_report.pdf

5. Laxmi Sharma, *GDPR: After 25th May, What Medium And Long-Term Actions?* (2018, June 6). Retrieved from https://www.smartdatacollective.com/gdpr-25th-what-medium-long-term-actions/

6. Daniel Mintz, *The Road to Becoming GDPR Compliant Leads to Log Term Success*, (2018, October 12). Retrieved from: http://www.dataversity.net/road-becoming-gdpr-compliant-leads-long-term-success/

7. John Tomaszewski, *"Opening Clauses" in the GDPR – It Might Not Be As Easy As We Thought*, (2017, July 3). Retrieved from: *https*://www.globalprivacywatch.com/2017/07/opening-clauses-and-the-gdpr-it-might-not-be-as-easy-as-we-thought/

8. Lei Shen, Rebecca Eisner, *Updating Your Vendor Agreements to Comply With GDPR,* (2017, March 28). Retrieved from:
https://iapp.org/news/a/updating-your-vendor-agreements-to-comply-with-gdpr/

9. Recital 26 EU GPDR, (2016). Retrieved from:
http://www.privacy-regulation.eu/en/recital-26-GDPR.htm

10. How To Monetize Your Data? Conducted by Lotame, (2018, February 20). Retrieved from:
https://www.lotame.com/how-to-monetize-your-data/

11. Elizabeth Kemery Sipes, Bryan Cave, Joshua James, *Current data security issues for financial services firms,* (2016). Retrieved from:
https://www-emeraldinsight-com.ezp.skema.edu/doi/full/10.1108/JOIC-07-2016-0034

12. Agile GDPR Compliance Management: An End-To-End Process leveraging Artificial Intelligence. (2018, July 12). Retrieved from https://blog.confidentgovernance.com/2018/07/12/agile-gdpr-compliance-management-an-end-to-end-process-leveraging-artificial-intelligence/

13. Do you need to hire a DPO? - Talentarc. (2018, May 14). Retrieved from https://getconga.com/contract-management/*

14. Ivey, V. (2013, December 16). 5 Tips to Keep Your Data Secure on the Cloud. Retrieved from https://www.cio.com/article/2380182/cloud-security/5-tips-to-keep-your-data-secure-on-the-cloud.html

15. GDPR & Contract Management? 5 Must-Have Features. (2018, September 7). Retrieved from https://precisely.se/2018/04/18/gdpr-contract-management/

16. Gatekeeper. (n.d.). Gatekeeper Contract Management. Retrieved from https://www.gatekeeperhq.com/contract-management-lp?utm_source=capterra&utm_medium=cpc&utm_term=contract-management&utm_content=v1&utm_campaign=capterra-contract-mgmt&capchannel=GetApp

17. Current data security issues for financial services firms (2016), Emerald Group Publishing Limited. Retrieved from https://www-emeraldinsight-com.ezp.skema.edu/doi/full/10.1108/JOIC-07-2016-0034

18. Art. 17 GDPR? Right to erasure ('right to be forgotten?) | General Data Protection Regulation (GDPR). (n.d.). Retrieved from https://gdpr-info.eu/art-17-gdpr/

19. Is Your Company Ready for a Big Data Breach? Sponsored by Experian® Data Breach Resolution, conducted by Ponemon Institute, (2013, April) http://www.experian.com/assets/data-breach/brochures/2014-ponemon-2nd-annual-preparedness.pdf

20. Current data security issues for financial services firms (2016) Emerald Group Publishing Limited. Retrieved from: https://www-emeraldinsight-com.ezp.skema.edu/doi/full/10.1108/JOIC-07-2016-0034

21. Agile GDPR Compliance Management: An End-To-End Process leveraging Artificial Intelligence. (2018, July 12). Retrieved from https://blog.confidentgovernance.com/2018/07/12/agile-gdpr-compliance-management-an-end-to-end-process-leveraging-artificial-intelligence/

22. Fines and Penalties – GDPR EU.org. (n.d.). Retrieved from
https://www.gdpreu.org/compliance/fines-and-penalties/

23. Comparing the Benefits of Pseudonymization and Anonymization Under the GDPR, https://iapp.org/media/pdf/resource_center/PA_WP2-Anonymous-pseudonymous-comparison.pdf

24. Guild of Project Controls Compendium and Reference *(CaR) – 10.3.3.7 Multi-Attribute Decision Making* - Planning Planet (2015 November). Retrieved from: http://www.planningplanet.com/guild/gpccar/managing-change-the-owners-perspective

25. Marks, G. (2014, June 23). 7 Ways To Protect Yourself Against A Data Breach. Retrieved from https://www.forbes.com/sites/quickerbettertech/2013/12/31/7-ways-to-protect-yourself-against-a-data-breach/#

26. What is mobile device management (MDM)? - Definition from WhatIs.com. (n.d.). Retrieved from https://searchmobilecomputing.techtarget.com/definition/mobile-device-management

27. Marks, G. (2014, June 23). 7 Ways To Protect Yourself Against A Data Breach. Retrieved from: https://www.forbes.com/sites/quickerbettertech/2013/12/31/7-ways-to-protect-yourself-against-a-data-breach/#

28. GDPR: After 25th May, What Medium And Long-Term Actions? (2018, June 8). Retrieved from: https://www.smartdatacollective.com/gdpr-25th-what-medium-long-term-actions/

29. The price of free: how Apple, Facebook, Microsoft and Google sell you to advertisers. (2015, October 1). Retrieved from: https://www.pcworld.com/article/2986988/privacy/the-price-of-free-how-apple-facebook-microsoft-and-google-sell-you-to-advertisers.html

30. U.S. Facebook advertising revenue 2018, produced by Statistic. (2018). Retrieved from: https://www.statista.com/statistics/544001/facebooks-advertising-revenue-worldwide-usa/

31. Ivey, V. 5 Tips to Keep Your Data Secure on the Cloud. (2013, December 16). Retrieved from: https://www.cio.com/article/2380182/cloud-security/5-tips-to-keep-your-data-secure-on-the-cloud.html

32. GDPR & Contract Management? 5 Must-Have Features. (2018, September 7). Retrieved from: https://precisely.se/2018/04/18/gdpr-contract-management/

33. APMP International. (n.d.). *Agile Project Management*. Retrieved from: https://www.trainingbytesize.com/?lang=fr

34. Agile CRM - GDPR Compliance. (n.d.). Retrieved from: https://www.agilecrm.com/gdpr-compliance

35. GDPR – Threat or Opportunity? – We are Lean and Agile. (n.d.). Retrieved from: https://weareleanandagile.com/uncategorized/gdpr-threat-or-opportunity/

36. Time-Saving Methods to Prioritise Your GDPR Compliance. Produced by Nymity (2018, August 10). Retrieved from: http://blog.nymity.com/blog/time-saving-methods-to-prioritise-your-gdpr-compliance

37. France: Pragmatism and Flexibility for the GDPR Implementation | Password Protected. (2018, February 20). Retrieved from: https://www.passwordprotectedlaw.com/2018/02/france-pragmatism-and-flexibility-for-the-gdpr-implementation/

38. GDPR Compliance Monitoring. (2018, June 12). Retrieved from: https://www2.deloitte.com/mt/en/pages/risk/articles/mt-risk-article-gdpr-monitoring.html

39. GDPR and the Road to Increased Customer Loyalty and Trust - Security Thinking Cap. (2018, June 12). Retrieved from: https://securitythinkingcap.com/gdpr-increase-customer-loyalty-trust/

40. GDPR Best Practices Implementation Guide. (n.d.). Retrieved from https://www.infosecurityeurope.com/__novadocuments/355669?v=636289786574700000

About the Author

Etienne Plassard

Paris, France

Etienne Plassard is a Master 2 graduate student in Project Management with one year of professional experience in recruitment and project management. Born in Côte d'Or in France, he studied mathematics, geography and economy in France, and then entered SKEMA Business School in Lille, France. He studied capital markets and accountability in Canada for 6 months, and then went to Brazil to study project management. He has been accredited PRINCE2 and AgilePM in December 2018. He is currently working for a consulting firm as a Business technology & integration consultant in Paris. He is publishing his first Student Paper under the tutorage of Dr Paul D. Giammalvo, CDT, CCE (#1240), MScPM, MRICS, Senior Technical Advisor (Project Management) to PT Mitratata Citragraha. (PTMC), Jakarta, Indonesia.

Etienne lives in Paris, France and can be contacted at etienne.plassard@hotmail.fr