

General Data Protection Regulation: How to Write Best Data Privacy Policy^{1, 2}

Alexandra Klébé

ABSTRACT

On May 2018, the European Commission enforced the law about personal information protection with the General Data Protection Regulation (GDPR). Indeed, it brings several improvements in data protection but could be seen as an obstacle for companies which business is based on the collection and use of personal information. The aim of this paper is to give best practices to these companies to still maintain their business while respecting the new regulation. By following both qualitative and quantitative methods, it will be present clauses that must be taken as an example for the concerned companies so that they would write and apply proper data privacy clauses.

Keywords - Personal information, Contracts, Data privacy, Privacy policy, Collection, GDPR, Project Management

INTRODUCTION

“On Friday, September 28th, Facebook forced 90 million users to log out as a safety measure”³. Indeed, it has been attacked by hackers who had exploited a breach to break into users’ accounts. The hackers tried to collect private information from 50 million accounts, such as name, sex, and hometown. This happens barely four months after the European Commission enforced the law about personal information protection with the General Data Protection Regulation (GDPR) on May 2018.

Actually, the European Commission decided to reinforce data privacy through the GDPR in May 2018 for the protection of personal data for Europeans inside and outside the EU. It brings several improvements over the Data Protection Act 1998. Here are some of them. First, privacy policies

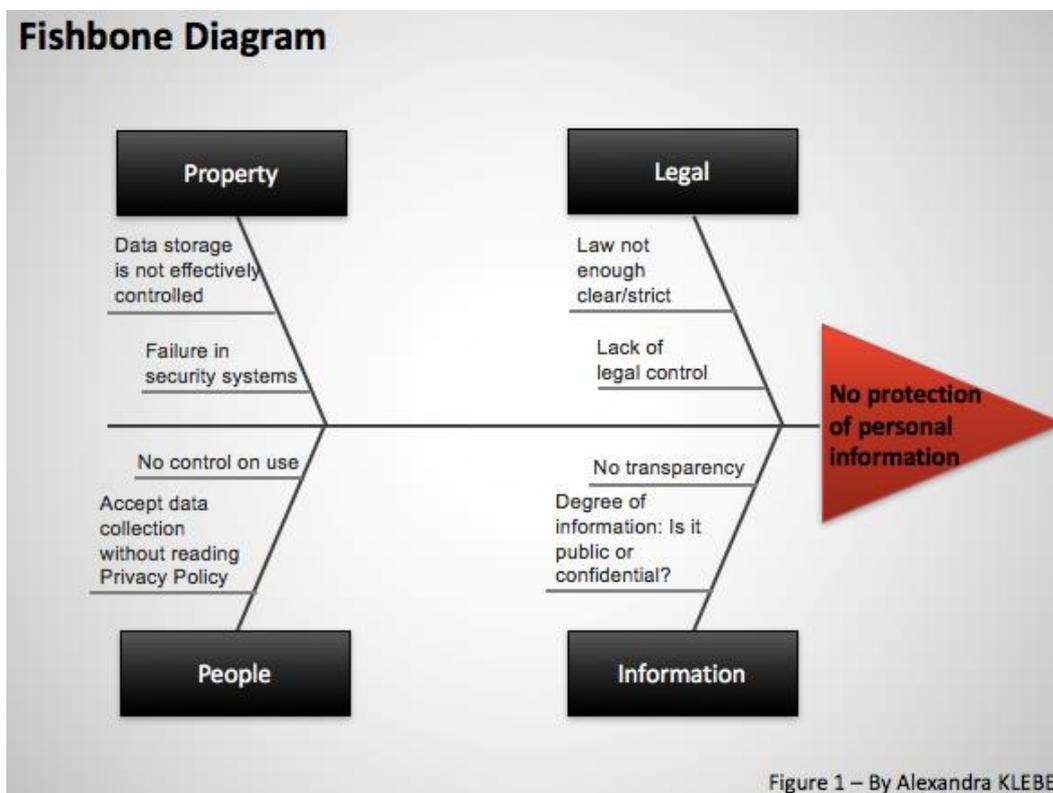
¹ Editor’s note: Student papers are authored by graduate or undergraduate students based on coursework at accredited universities or training programs. This paper was prepared for the course “International Contract Management” facilitated by Dr Paul D. Giammalvo of PT Mitratata Citragraha, Jakarta, Indonesia 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: Klébé, A. (2019). General Data Protection Regulation: How to Write Best Data Privacy Policy, *PM World Journal*, Vol. VIII, Issue V, June.

³ Isaac, M., & Frenkel, S. (2018, September 28). Facebook Security Breach Exposes Accounts of 50 Million Users. *The New York Times*. <https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html>

will have to be written in a clear and straightforward language, no more complicated terms. Businesses will also have to collect affirmative consents from users for using their data, silence is no longer consent. The GDPR claims for more transparency: users have to know when their data is transferred outside the EU, and collection of data has to be done for only a well-defined purpose. The GDPR also enforces users' rights about information, data transfer, and access, and give them a clearly defined 'right to be forgotten' – data can be deleted easily. Last but not least, it offers stronger enforcements such as fines when businesses violate the rules.⁴

However, even if companies have to follow new rules, data protection is still a current issue as proven by the Facebook incident on September. Indeed, a lot of concerns remain as presented in the fishbone diagram below⁵:



There are many issues about data privacy - especially about the collection and use of personal information - companies should be aware of when conducting projects. Let's remind here that, according to Max Wideman's Comparative Glossary, a project is: 'A novel undertaking

⁴ European Commission. A new era for data protection in the EU (n.d.). Retrieved from https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-changes_en.pdf

⁵ By Author. *Fishbone Diagram*.

or systematic process to create a new product or service the delivery of which signals completion. Projects involve risk and are typically constrained by limited resources.’⁶

Integrating GDPR new rules have forced companies to rethink the process when conducting a project and taking more into account the protection of personal information when collecting and using it. Let’s not forget that users are involved too. For example, when the GDPR has been implemented, companies had to warn people about changes in their privacy policies and to get an affirmative consent. This is why users have received lots of emails from websites they had already subscribed and have to click on an agreement box when connecting to a new one. However, lots of people have accepted and are still accepting new general conditions without even reading them or knowing about what GDPR is and how it actually protect them. To resume, both sides - companies and users – have a common issue about privacy policy.

Step1- Problem definition

Let’s focus on companies’ side, and particularly on how project managers are challenged by these new rules on their day-to-day job - when information is their working base - by answering this:

- What are the best practices for guaranteeing the protection of personal information?
- Is data privacy always well ensured explicitly?
- How can companies ensure customers that their data is kept safe?

METHODOLOGY

In order to proceed to this analysis, let’s use the Multi-Attribute Decision Making (MADM) methods. It will be interesting to combine two approaches: a non-compensatory approach, which is the dominance technique, and a compensatory approach, which is the weighting technique.

Step2- Feasible alternative solutions

In this paper, it will be considered five feasible alternatives for the protection of personal information in business projects contracts, which are the followings:

- Microsoft privacy clauses
- Google privacy clauses
- Apple privacy clauses
- Facebook privacy clauses
- Amazon privacy clauses

⁶ Wideman Comparative Glossary of Project Management Terms v5.5. (n.d.). Retrieved from http://www.maxwideman.com/pmglossary/PMG_P12.htm - Project

All these alternatives must be analyzed in order to define what makes a proper clause that ensures customers' data are kept safe. Let's use the six data protection principles in Article 5 of the GDPR⁷ to help in determining the scoring attributes to conduct the study:

- Lawfulness
- Fairness
- Transparency
- Purpose limitation
- Data minimization
- Accuracy
- Reliability⁸
- Precision
- Storage limitation
- Integrity and confidentiality

Step3- Development of the feasible alternatives

As the first alternative solution, let's consider the Microsoft clause 'You own and control your data'⁹ in the Privacy Overview of the Microsoft Trust Center. In this clause, Microsoft ensures that privacy is protected because they committed giving customers control over the collection, use, and distribution of their data. They assure to be transparent about policies, operational practices, and technologies that keep data private. They also limit the use of data to what was agreed by customers and remove data from systems when no more necessary. Microsoft allows their customers to know in which geographic location data is maintained and complies with international data protection laws to do so. They have implemented measures to protect data from inappropriate access, including limits for Microsoft personnel.

For the second alternative, Google has a clause named 'Keeping your information secure'¹⁰ in its Privacy Policy which explains how customers' information is protected. Google ensures the protection of customers' data against unauthorized accesses, alteration, disclosure, destruction of information kept by Google. For doing so, Google uses encryption while data transit; security features; review of the information collection, storage, and processing practices; and restricted access to people who need the information to process it. All other aspects of data privacy need to be managed directly by the customers themselves – as explained in the whole contract, such

⁷ IT Governance Privacy Team (2017). Chapter4: Six Data Protection Principles. In *EU General Data Protection Principles (GDPR). An Implementation and Compliance Guide* (2nd ed.).

Retrieved from

<https://books.google.fr/books?hl=fr&lr=&id=hnQ2DwAAQBAJ&oi=fnd&pg=PA1&dq=data+privacy+clause+gdpr&ots=WiJdxsSYYv&sig=ughORIUG-ucVInExl5euL1Z0I5M - v=onepage&q&f=false>

⁸ GUILD OF PROJECT CONTROLS COMPENDIUM and REFERENCE (CaR) | Project Controls - planning, scheduling, cost management and forensic analysis (Planning Planet). (n.d.). Retrieved from <http://www.planningplanet.com/guild/gpccar/introduction-to-managing-cost-estimating-budgeting%20Figure%201>

⁹ Microsoft Trust Center. Privacy Overview (2018). Retrieved from <https://www.microsoft.com/en-us/trustcenter/privacy>

¹⁰ Google. Privacy Policy – Privacy & Terms. (Last Updated: 2018, May 25). Retrieved from <https://policies.google.com/privacy?hl=en#infochoices>

as in the ‘Your privacy controls’ clause. They can have some guidance from Google assistance, but they have to do the processes on their own.

The third alternative is Apple clause ‘Protection of personal information’¹¹ from the Policy Privacy. Such as Google, Apple protects customers’ personal information during transit using encryption and also when it is stored by using computer systems with limited access. However, when customers’ share personal information and content, it is visible by other users and can be read, collected, and used by them. Apple recommends to take care of what customers are actually publishing. Apple also mentions Family share by informing that third party with access to Family share could download everything that was shared on it.

The fourth alternative chosen is from Facebook Data Policy, with the following ‘How can you exercise your rights provided under the GDPR?’ and ‘Data retention, account deactivation and deletion’¹². Facebook gives customers’ the right to access, rectify, port and erase data. Customers’ also have the right to object and restrict certain processing of their data, by unsubscribing for example. Facebook assures also that data is stored until it is no longer necessary – or when the account is deleted. For example, search history is deleted after six months.

The last alternative is from Amazon.com Privacy Notice ‘How secure is information about me?’¹³ Customers’ information is kept safe during transmission by encrypting it. Only last four digits of the credit card number are revealed during an order – but the entire credit card number is given to the credit card company during order processing. Amazon.com warn its customers that unauthorized access to password may happen and advise them to sign off once done on the website.

After all these explanations, it seems that Microsoft has the most complete clause ensuring data privacy, but let’s examine and score each one of the alternatives.

Step4- Selection of the criteria to accept or reject the alternative solutions

In order to evaluate each alternative more precisely, let’s use a non-compensatory approach of MADM called the dominance technique¹⁴.

¹¹ Apple. Legal - Privacy Policy. (Last Updated: 2018, May 22). Retrieved from <https://www.apple.com/legal/privacy/en-ww/>

¹² Facebook. Data Policy. (Last Updated: 2018, April 19). Retrieved from <https://www.facebook.com/about/privacy>

¹³ Amazon.com Help: Amazon.com Privacy Notice. (Last Updated: 2017, August 29). Retrieved from https://www.amazon.com/gp/help/customer/display.html/ref=asus_gen_not?ie=UTF8&nodeId=468496&Id=NSGoogle#GUID-1B2BDAD4-7ACF-4D7A-8608-CBA6EA897FD3_SECTION_277A1D99140544EE9259ACA749AE3C3D

¹⁴ Sullivan, Wickes & Kroelling (2014) Engineering Economics 15th Edition

Let's first be more specific about the chosen attributes¹⁵ & ¹⁶:

- Transparency: 'the data subject must be told what processing will occur'
- Fairness: 'the processing must match this description'
- Lawfulness: 'the processing must be for one of the purposes specified in the Regulation'.
- Purpose limitation: the company 'must define up front what the data will be used for and limit the processing to only what is necessary to meet that purpose'.
- Data minimization: the company 'should hold no more data beyond what is strictly required'.
- Accuracy: the company 'need to ensure that it has processes in place to keep all personal data accurate and up to date'.
- Reliability: the degree to which the company can be trusted.
- Precision: the company is very precise about data safety.
- Storage limitation: 'if the company no longer need the data, it should get rid of it'.
- Integrity and confidentiality: 'personal data must be classified as confidential even within the organization'

The following table is the MADM results after a qualitative analysis of the five alternatives. For building the table of dominance, let's use the following code:

- Green: attribute is fully taken into account;
- Yellow: attribute is considered but still vague;
- Red: no mention of the attribute.

	Microsoft	Google	Apple	Facebook	Amazon.com
Transparency	Better	Equal	Equal	Better	Worse
Fairness	Better	Equal	Equal	Better	Worse
Lawfulness	Better	Worse	Worse	Worse	Worse
Purpose limitation	Better	Worse	Worse	Worse	Equal
Data minimization	Better	Worse	Worse	Worse	Equal

¹⁵ IT Governance Privacy Team (2017). Chapter4: Six Data Protection Principles. In *EU General Data Protection Principles (GDPR). An Implementation and Compliance Guide* (2nd ed.).

Retrieved from

<https://books.google.fr/books?hl=fr&lr=&id=hnQ2DwAAQBAJ&oi=fnd&pg=PA1&dq=data+privacy+clause+gdpr&ots=WiJdxsSYYv&sig=ughORIUG-ucVInEx15euL1Z0I5M - v=onepage&q&f=false>

¹⁶ GUILD OF PROJECT CONTROLS COMPENDIUM and REFERENCE (CaR) | Project Controls - planning, scheduling, cost management and forensic analysis (Planning Planet). (n.d.). Retrieved from

<http://www.planningplanet.com/guild/gpccar/introduction-to-managing-cost-estimating-budgeting%20Figure%202011>

Accuracy	Worse	Equal	Worse	Equal	Equal
Reliability	Equal	Equal	Worse	Equal	Equal
Precision	Equal	Better	Equal	Equal	Better
Storage limitation	Better	Better	Worse	Better	Worse
Integrity and confidentiality	Better	Better	Better	Worse	Better

Figure 2. Table of dominance, quantitative analysis¹⁷

According to the table of dominance, the best alternative is Microsoft clause ‘You own and control your data’ whereas the worse one seems to be Apple clause ‘Protection of personal information’.

Step5- Analysis, and comparison of the alternatives

Even if Figure 2 seems to show that Microsoft privacy clauses are the best alternative, let’s conduct a quantitative analysis to confirm that.

We will conduct this analysis by scoring each of our alternatives following a precise rule:

- Green = 1
- Yellow = 0.5
- Red = 0

	Microsoft	Google	Apple	Facebook	Amazon.com
Transparency	1	0.5	0.5	1	0
Fairness	1	0.5	0.5	1	0
Lawfulness	1	0	0	0	0
Purpose limitation	1	0	0	0	0.5
Data minimization	1	0	0	0	0.5
Accuracy	0	0.5	0	0.5	0.5
Reliability	0,5	0.5	0	0.5	0.5
Precision	0,5	1	0.5	0.5	1
Storage limitation	1	1	0	1	0

¹⁷ By Author, *Table of dominance*.

Integrity and confidentiality	1	1	1	0	1
Sum	8	5	2.5	4.5	4

Figure 3. Quantitative analysis¹⁸

Thanks to this new scored ranking, let's conduct a compensatory approach of MADM which is the additive weighting technique.

Attributes	Step1	Step2		Microsoft		Google		Apple		Facebook		Amazon.com	
	Relative rank	Normalized weight (A)	(B)	(A)x(B)	(C)	(A)x(C)	(D)	(A)x(D)	(E)	(A)x(E)	(F)	(A)x(F)	
Transparency	1	1/55 = 0.018	1	0.018	0.5	0.009	0.5	0.009	1	0.018	0	0	
Fairness	6	6/55 = 0.109	1	0.109	0.5	0.055	0.5	0.055	1	0.109	0	0	
Lawfulness	4	4/55 = 0.073	1	0.073	0	0	0	0	0	0	0	0	
Purpose limitation	2	2/55 = 0.036	1	0.036	0	0	0	0	0	0	0.5	0.018	
Data minimization	7	7/55 = 0.127	1	0.127	0	0	0	0	0	0	0.5	0.064	
Accuracy	5	5/55 = 0.091	0	0	0.5	0.046	0	0	0.5	0.046	0.5	0.046	
Reliability	3	3/55 = 0.055	0.5	0.028	0.5	0.014	0	0	0.5	0.014	0.5	0.014	
Precision	8	8/55 = 0.145	0.5	0.073	1	0.145	0.5	0.073	0.5	0.073	1	0.145	
Storage limitation	10	10/55 = 0.182	1	0.182	1	0.182	0	0	1	0.182	0	0	
Integrity and confidentiality	9	9/55 = 0.164	1	0.164	1	0.164	1	0.164	0	0	1	0.164	
SUM	55	1	8	0.81	5	0.615	2.5	0.301	4.5	0.442	4	0.451	

This provides a strong and powerful ranking order for our five feasible alternatives.

¹⁸ By author, *Quantitative analysis*

Step 6- Selection of the preferred alternative

The previous table clearly shows and confirms the first assumption of this paper. Indeed, the **Microsoft privacy clauses** is by far the best standard ensuring customers' data privacy. It was shown by both qualitative and quantitative analysis.

Google privacy policies contain interesting clauses, but need to be improved to be considered as really efficient in data privacy because they still lack precision.

Step 7- Performance monitoring and post-evaluation of results

The methodology and the six precedent steps allow concluding that the best alternative is the Microsoft privacy clauses. Indeed, over the ten attributes chosen, it fully takes into account seven of them, such as transparency, purpose limitation and lawfulness. It ensures that personal information is protected and gives important information to customers about how their data are kept safe.

Moreover, some others are on the right path to do the same, but they still lack some critical aspects or omit them. For example, this is the case of Google, Amazon.com, and Facebook.

CONCLUSION

Since the European Commission enforced the law about personal information protection with the General Data Protection Regulation (GDPR) on May 2018, it is right for project, programme and portfolio managers to wonder how they can still have access to information and keep it safe while respecting the GDPR. This is why this paper tried to guide them by presenting what are the best practices to ensure the protection of personal information and keep customers' private data safe once collected.

For doing so, Microsoft, Google, Apple, Facebook, and Amazon.com privacy clauses have been compared according to ten attributes, among them the six principles of the GDPR. After following both qualitative and quantitative methods, it appears that Microsoft privacy clauses are the best alternative and can be taken as a model for the redaction and application of future data privacy clauses.

BIBLIOGRAPHY

Isaac, M., & Frenkel, S. (2018, September 28). Facebook Security Breach Exposes Accounts of 50 Million Users. *The New York Times*.
<https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html>

European Commission. 2018 reform of EU data protection rules (2018,9). Retrieved from https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

European Commission. Model contracts for the transfer of personal data to third countries. (2018, January 8). Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en

European Commission. Data protection. (2018, January 8). Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection_en

European Commission. A new era for data protection in the EU (n.d.). Retrieved from https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-changes_en.pdf

Wideman Comparative Glossary of Project Management Terms v5.5. (n.d.). Retrieved from http://www.maxwideman.com/pmglossary/PMG_P12.htm - Project

Information Commissioner's Office. Model Contract Clauses. International Transfers of Personal Data. From https://ico.org.uk/media/for-organisations/documents/1571/model_contract_clauses_international_transfers_of_personal_data.pdf

Microsoft Trust Center. European Union Model Clauses (n.d.). Retrieved from <https://www.microsoft.com/en-us/TrustCenter/Compliance/EU-Model-Clauses>

Pegarella, S. (2018, October 30). GDPR Privacy Policy. Retrieved from <https://termsfeed.com/blog/gdpr-privacy-policy/>

TermsFeed. How to Update Your Existing Privacy Policy for GDPR Compliance. (2018, September 21). Retrieved from <https://termsfeed.com/blog/gdpr-compliance-update-privacy-policy/>

Mackie, J. (2017, July 14). What Makes a Good Privacy Policy. Retrieved from https://termsfeed.com/blog/good-privacy-policy/#Essential_clauses_for_the_Privacy_Policy

Davis, B. (2017, July 17). GDPR: How to create best practice privacy notices (with examples). Retrieved from <https://econsultancy.com/gdpr-best-practice-privacy-notices-examples/>

FactSet Research Systems Inc. (Last Updated: March 2017). Privacy Policy and Legal Statements. Retrieved from <https://www.factset.com/privacy>

Mackie, J. (2018, March 10). How to Write a Privacy Policy. Retrieved from <https://termsfeed.com/blog/write-privacy-policy/>

IT Governance Privacy Team (2017). Chapter4: Six Data Protection Principles. In *EU General Data Protection Principles (GDPR). An Implementation and Compliance Guide* (2nd ed.).

Retrieved from

<https://books.google.fr/books?hl=fr&lr=&id=hnQ2DwAAQBAJ&oi=fnd&pg=PA1&dq=data+privacy+clause+gdpr&ots=WiJdxsSYYv&sig=ughORIUG-ucVInExl5euL1Z0I5M-v=onepage&q&f=false>

GUILD OF PROJECT CONTROLS COMPENDIUM and REFERENCE (CaR) | Project Controls - planning, scheduling, cost management and forensic analysis (Planning Planet). (n.d.). Retrieved from <http://www.planningplanet.com/guild/gpccar/introduction-to-managing-cost-estimating-budgeting%20Figure%201>

Microsoft Trust Center. Privacy Overview (2018). Retrieved from <https://www.microsoft.com/en-us/trustcenter/privacy>

Google. Privacy Policy – Privacy & Terms. (Last Updated: 2018, May 25). Retrieved from <https://policies.google.com/privacy?hl=en#infochoices>

Apple. Legal - Privacy Policy. (Last Updated: 2018, May 22). Retrieved from <https://www.apple.com/legal/privacy/en-ww/>

Facebook. Data Policy. (Last Updated: 2018, April 19). Retrieved from <https://www.facebook.com/about/privacy>

Amazon.com Help: Amazon.com Privacy Notice. (Last Updated: 2017, August 29). Retrieved from https://www.amazon.com/gp/help/customer/display.html/ref=asus_gen_not?ie=UTF8&nodeId=468496&ld=NSGoogle#GUID-1B2BDAD4-7ACF-4D7A-8608-CBA6EA897FD3_SECTION_277A1D99140544EE9259ACA749AE3C3D

Sullivan, Wickes & Kroelling (2014) Engineering Economics 15th Edition

About the Author



Alexandra Klébé

Paris, France



Alexandra Klébé is a MSc Project and Programme Management & Business Development student at SKEMA Business School, Paris. Born at Paris, she integrated SKEMA Business School Lille on the results of an entrance examination. In her school, she took the opportunity of living abroad in both Brazil, Belo Horizonte and the United States, Raleigh. Coming back to France, she worked as an Assistant Project Manager in a design agency where she was in collaboration with French, Europeans, and International brands. Ending her studies, she is actually writing a thesis before graduation.

Alexandra lives in Paris, France and can be contacted at alexandra.klebe@skema.edu