Best practices for data privacy clause in Saas Agreements[1]

Amélie Tonneau

ABSTRACT

The explosion of IT leaks and cyber-security attacks have risen the concerns from governments and Software-as-a-service (Saas customers' which currently feel unsafe regarding the processing and the protection of the data they share and give access to their Saas suppliers. The objective of this report is to understand the different requirements from the current and new General Data Protection Regulation (GDPR) legislation regarding the matter of data privacy. This paper is based on a qualitative study using a multi-attribute decision-making and fishbone methods, websites and articles analysis.

Even though the legislation is changing, many medium-sized companies are yet not aware of these requirements they should comply with. Bear in mind that the new requirements will be mandatory to comply with on May 2018. This will lower Saas providers' flexibility in terms of processing but increase Saas customers' protection.

The different alternatives or requirements from both regulation will be analysed and therefore show you that a mix of requirements are necessary to draft the best data privacy clause for your next Saas agreements and to protect your customers.

Key words: Software-as-a-Service (Saas), data privacy, IT security, legislation, confidentiality

INTRODUCTION

In a fast global changing environment, the Software-as-a-Service (Saas) industry is currently booming, expecting to reach $112.8 billion by 2019. Considered as a precise software distribution model, Saas providers use a third-party to host their applications on the Cloud, making their applications directly available to users over the Internet. With a significant decrease in cloud third-party prices, more and more small businesses are nowadays using Saas in order to boost sales and productivity.

[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 as a deliverable 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*.*

While many Saas companies use collected data from their customers to help their growth, which might be very sensitive data, Saas agreements need to provide precise Data Privacy clauses. These data privacy clauses cover the requirements and obligations from the provider regarding data collection and their means for keeping their customers' data secure. Unfortunately, current trends have shown that Saas providers are currently failing in keeping customers aware of their rights regarding the confidentiality of their own data. In this difficult context, choosing the right provider by evaluating risks should become a common practice from a customer point of view if Saas agreements don't improve transparency. Before signing-up with Cloud computing services, companies and/or individuals will have now to think if the data they are giving up is confidential and to which extend.

In a context where IT security and cyber-attacks are consequently increasing, drafting Saas Agreements & their Data privacy clauses might be a challenge for small businesses. In a changing legal environment in the EU, what should a data privacy clause contains? What are the advantages of the new GDPR regulation?

In the following you will be able to understand the current trends about Data Privacy clauses in within the Saas industry. Then, we will raise the question of legal requirements and the new legislation in the European Union that will come into effect in May 2018. Finally, we will recommend you the best Data privacy clause for your business.

METHODOLOGY

2. Development of feasible alternatives

In order to draft the best data privacy clause, we will have to understand the different alternatives that we are currently facing in this period of changing legislation. We will therefore go into details regarding data privacy clause under current national directives from the European Union and the Data privacy clauses under the new GDPR legislation that will come into effect in May 2018. It is important to say that currently Saas suppliers have only few obligations regarding their customers when it comes to data processing. The new regulation will completely change and standardize the status of legal obligations.

In both alternatives, Saas agreements determine if suppliers are processing data on behalf of its customers or as a data (acting as a processor) or data controller on its own. In most Saas agreement, the suppliers act as data processor. This will be part of the data Privacy included in the Master Service Agreement (reserved from Licensing Agreement for real software company). It will enable the provider to protect itself against a third party but also from the data controller point of view if the supplier would be processing his data against regulation.

CURRENT DATA PRIVACY & PROCESSING CLAUSE

Until the 18th of May 2018, Saas suppliers from the European Union use their own directive to draft their data privacy clause. For instance, the UK is regulated under Data Protection Act (DPA) from 1998 and France under the "Informatiques & Libertés" law. No European standards apply here which make the situation quite difficult in a globalized world. Under the current legislation the data controller or Saas customers are mainly responsible for complying with the local requirements.

What are the current controllers' (or customers) rights?

- Access a copy of their personal data collected
- Refuse collection of data likely to cause damages
- Refuse collection if the purpose of collection is for direct marketing
- Refuse automation means
- Claim for rectification or deletion in case of inaccurate data
- Claim compensation in case of not following legal regulation regarding data collection & processing

Alternatives as current practices regarding data privacy and processing:

1. Customer compliance

Customer compliance on data protection: With current European legislations, it is the responsibility of Saas customers to make sure that the suppliers is complying with the followings: "Their data must be: fairly and lawfully processed; processed for limited purposes; adequate, relevant and not excessive; kept for no longer than necessary; processed in accordance with the data subject's rights; secure; and transferred outside of the EEA only if there is adequate protection in that country."[1]. Bear in mind that Saas providers are meant to follow the Saas customers' instructions. Both parties should protect themselves knowing this by communicating clearly the mentions above into the data privacy and processing clause.

Data Processing: Saas customers are entirely responsible for using Saas services therefore customers are responsible for the data they are giving authorization to the provider. Most of the time, the customers are still considered as the owners of their data while being processed by the processor. Therefore the Saas provider will be held responsible in case data is not meeting conformity standards, laws and directives regarding local regulation.

Data Security: As the customers are held responsible for their own personal data, they are also responsible for ensuring that they insert obligated measures into the clause if needed. For instance, requiring encryption while processing confidential data.

2. Subject Access Request: Saas customers have currently the right to claim and request a copy regarding the information being collected and held from the suppliers. A time limit as well as a releasing process should be added to the clause is which the customer can pretend to get his information at minimal cost. This is a legal obligation to Saas providers.

3. Transferring data outside the European Economic Area (EEA): A specific consent to the customers is required when the data is being transferred except if the country outside of the EEA has a similar data regulation.

4. Return of data: Saas providers are meant to give Saas customers their data back when the contract ends. The conditions of this return should be agreed formally in the data privacy clause. It is also possible from the Saas providers to enclose in the data privacy clause that they will charge a certain sum if they have to transfer the data to another provider.

NEW DATA PRIVACY AND PROCESSING CLAUSE UNDER THE GDPR LEGISLATION

In May 2018, the new GDPR legislation will change the contents and obligations from both Saas providers and Saas customers regarding the data privacy clause in their agreements.

What are the new controllers' (or customers) rights?

- Saas customers will have the right to data portability;
- Saas customers can have to right to be forgotten;
- Saas customer will have the opportunity to prevent profiling;
- Saas customers will be able to refuse to processing;
- Saas customers will be able to ask for rectification and erasure;
- Saas customers can ask for access requests ("SARs") of their data.

Alternatives as new practices regarding data privacy and processing:

5. Consent: From May 2018, it is required from Saas suppliers to give a detailed consent as well as an indication when it comes to the data processing process of their customers. For instance, a tick box telling the customer that their data will be processed when entering a website or an application.

[1] http://www.experian.co.uk/assets/responsibilities/brochures/dataprotectionguidev16.pdf

6. Regulator: Both customer and provider will be regulated by a single regulator which should be their main location in within the European Union.

7. Data Protection Officer or DPO: Every companies from the European Union collection data will have the requirements to assess a DPO which will be responsible for the collection of large or regular collection of data.

8. Records: Saas providers will have the legal obligation to keep records regarding the data they process.

9. Cyber-security leaks & attacks: The company processing data which will have a breach will have the legal obligation to report the leak to their regulator under 72 hours. Saas providers will have to report the breach to their customers which have data processed mainly if lead to a risk regarding their data rights. This applies except in the following case:

- If data has been encrypted so the another actor cannot read it
- Saas provider has already followed a special process which will remove the risk
- If public announcement has been made

10. Impact assessment: If a cyber-security attack or data breach occurs leading to high risks for customers' rights, the Saas provider will have to do an impact assessment "DPIAs".

Companies not following the above standards can get up to 4% of annual global turnover or up to 20m Euros penalty.

3. Development of the outcome and cash flow for each alternative

		ATTRIBUTES					
		Saas providers' protection	Saas customers' protection	European cooperation	Transparency	Shared responsibility	Penalties
ALTERNATIVES	Customer compliance (protection, processing, safety)	+	-	-	-	-	-
	Subject access request	+	+	-	+	+	-
	Transfer outside the EEA	+	+	-	+	+	-
	Return of data	+	+	-	+	+	-
	Consent	+	+	+	+	+	+
	Regulator	+	+	+	+	+	+
	DPO	+	-	+	+	-	+
	Notification obligation	-	+	+	+	-	+
	Impact assessment	-	+	+	+	-	+

- + : the alternative has shown best practices when it comes to the selected criterion
- - : the alternative has shown poor practices and hasn't entirely covered the subject of the selected criterion

4. Selection of criterion (criteria)

Saas providers' protection: Are the rights of the Saas suppliers enhanced? Are they well protected with the information enclosed in the data privacy clause into the Saas agreements?

Saas customers' protection: Are the rights of the Saas customers enhanced? Are they well protected with the information enclosed in the data privacy clause into the Saas agreements?

European cooperation: In an increased global world, is the regulation standardised into the European Union?

Transparency: Are all the information regarding data privacy and data processing well communicated into the data privacy clause?

Shared responsibility customers/providers: Are both parties involved equally in drafting the fairest data privacy clause?

Penalties: Are penalties for not complying with the legislation well-explained to both parties?

FINDINGS

5. Analysis and comparison of the alternatives

		ATTRIBUTES						
		Saas providers' protection	Saas customers' protection	European cooperation	Transparency	Shared responsibility	Penalties	TOTAL
ALTERNATIVES	Customer compliance (protection, processing, safety)	5	1	1	2	1	1	**1.8**
	Subject access request	4	5	1	4	4	1	**3.2**
	Transfer outside the EEA	4	4	1	4	4	1	**3**
	Return of	4	5	1	4	4	1	**3.2**

	data							
	Consent	4	5	5	4	3	5	**4.3**
	Regulator	5	5	5	5	3	5	**4.7**
	DPO	5	2	5	4	2	5	**3.8**
	Notification obligation	2	5	5	5	2	5	**4**
	Impact assessment	3	5	5	5	3	5	**4.3**

Our analysis helps us understand the different focus from the old and new regulation and weights the advantages and disadvantages of all principles.

The Customer compliance alternative which includes the data protection, processing and safety from the old legislation was unfortunately lacking customer protection as the responsibility was not shared between suppliers and customers even when the providers was using and processing the data for his activity. Therefore, the transparency of this process was not clear for customers.

Then, bear in mind that all alternatives from the old legislation (Customer Compliance, Subject access request, Transfer outside the EEA, Return of data) does not include European standardisation. It means that all countries are currently using their own legislation for those alternatives. Processes and obligations might therefore differ.

6. Selection of the preferred alternatives

In order to draw the best data privacy clause in regards of the new GDPR legislation, those are the principles your data privacy clause should cover:

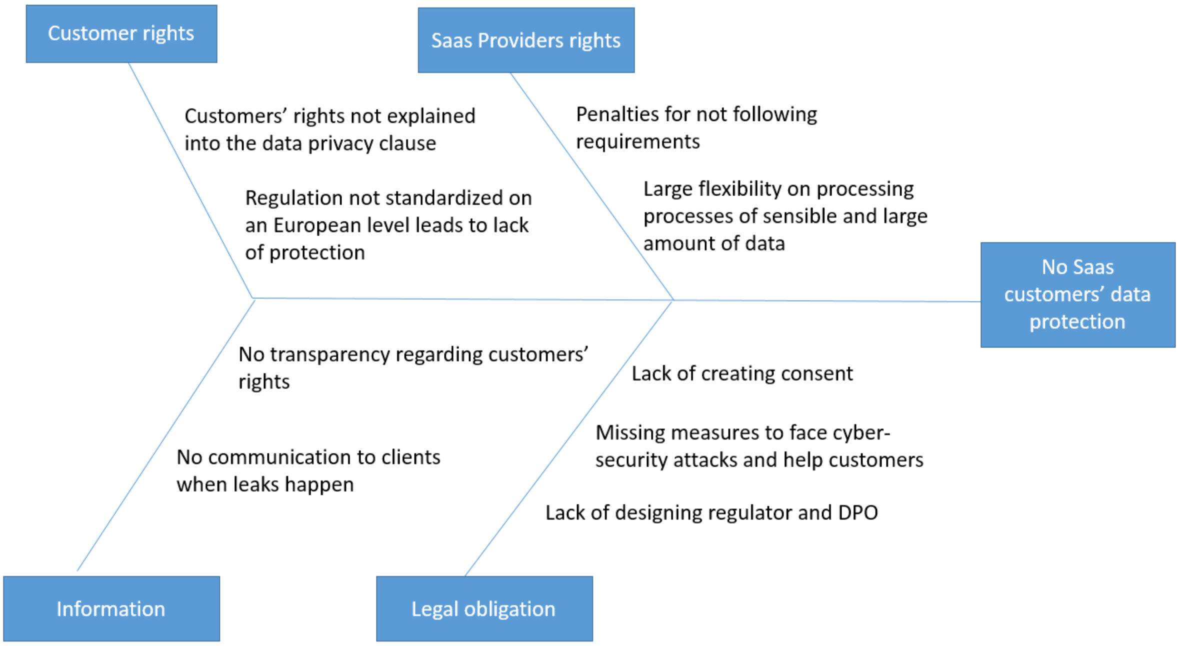
- Subject access request
- Transfer outside the EEA
- Return of data
- Consent
- Regulator
- DPO
- Notification obligation
- Impact assessment

Covering all aspects above is really important in order to create the fairest clause for your own protection and the ones from your clients. It will enable you to comply with the new regulation.

FOLLOW ON RESEARCH

7. Performance monitoring and post-evaluation of results

***Fishbone diagram**: risky alternatives induced from wrong use of the current GDPR regulation*


Customer rights
Saas Providers rights
Customers' rights not explained into the data privacy clause
Regulation not standardized on an European level leads to lack of protection
Penalties for not following requirements
Large flexibility on processing processes of sensible and large amount of data
No Saas customers' data protection
No transparency regarding customers' rights
No communication to clients when leaks happen
Lack of creating consent
Missing measures to face cyber-security attacks and help customers
Lack of designing regulator and DPO
Information
Legal obligation

The high flexibility given to Saas providers with the current legislation has created some doubts regarding the efficiency and the protection of Saas customer's rights.

Bear in mind that not following the new standards from the GDPR legislation will impact both customers and providers. In fact, customers will lack protection regarding their data but providers will also face serious penalties is they don't comply with the current principles.

CONCLUSION

The development of this new GDPR regulation will completely revolutionize the processes and ways current Saas companies collect their data but also improve protection. In fact, in a globalize world where IT leaks and cyber-attacks seem to be more and more frequent, companies and customers' need to be ready and know how to face these situations.

Bear in mind that the current legislation which is yet not standardized on an European level gives high flexibility to data processors which reduce the protection of customers' which should always feel safe moving on with a new provider.

Including the more information regarding the different principles described above will help you to comply with the new requirements but also will make your customers understand that you are up to date regarding security issues. Building trust is key to success.

BIBLIOGRAPHY

- *Charlotte Galichet (February 2017), Les nouvelles obligations des éditeurs de logiciels SaaS au regard du Règlement UE 2016/679 relatif à la protection des données à caractère personnel. Retrieved from http://avocatspi.com/2017/02/17/les-nouvelles-obligations-des-editeurs-de-logiciels-saas-au-regard-du-reglement-ue-2016679-relatif-a-la-protection-des-donnees-a-caractere-personnel/*
- *Maître Marion Depadt Bels, Protection des données : les sous-traitants & responsables de traitements sont-ils prêts pour le grand changement ?. Retrieved from http://www.cercle-editeurs.fr/securite-dans-le-cloud/dossier-editeurs-saas-et-gestion-des-donnees-personnelles-1-maitre-depadt-bels/*
- *Maxime, Captain Contrat (March 17), Les clauses présentes dans un contrat de logiciel SaaS. Retrieved from https://www.captaincontrat.com/articles-droit-commercial/contrat-logiciel-saas-clauses*
- *Irene Bodle (February 2017), SaaS Agreements – Data Protection – Amending EU Model Clauses. Retrieved from https://www.bodlelaw.com/saas/saas-agreements-data-protection-amending-eu-model-clauses*
- *Irene Bodle, SaaS Agreements (February 2016) – FAQs – EU Model Clauses, Retrieved from https://www.bodlelaw.com/saas/saas-agreements-faqs-eu-model-clauses*
- *Marie-Charlotte ROQUES-BONNET & Luis NETO GALVAO, LIABILITY FOR NON-COMPLIANCE*
- *WITH DATA PROTECTION OBLIGATIONS (January 2014). Retrieved from http://ec.europa.eu/justice/contract/files/expert_groups/final_draft_paper_dp_liability_en.pdf*
- *Andrew Solomon & Tom Cox, Kingsley Napley, Data Protection: 5 Things SaaS Providers Should do Today . Retrieved from https://www.lexology.com/library/detail.aspx?g=691efdd9-8721-4004-aedc-284fcc592962*
- *CNIL, Règlement européen sur la protection des données : ce qui change pour les professionnels. Retrieved from https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-ce-qui-change-pour-les-professionnels*

About the Author

Amélie Tonneau

SKEMA Business School
Paris, France

Amélie Tonneau is a Master's degree student at Skema Business School (Paris), Msc Project and Programme Management and Business Development (PPMBD). She joined Skema in 2014 in Lille and through those years developed her knowledge about different fields as Marketing, Law, Finance, Business development before stepping into project management. She had the opportunity to work in Spain, Belgium, and The Netherlands but also lived in Taiwan for a year. Passionate with Tech trends and start-ups' innovative ideas, she developed her professional experiences through different experiences in Sales and Marketing in Software as a Service (Saas) companies.