LGPD and gaming companies: main compliance aspects to Brazil´s General Data Protection Law

Laiane M. Caetano Fantini
Faculdade Mineira de Direito
PPGD PUC Minas/ CAPES
Belo Horizonte, Brazil
laianemaris@gmail.com

***Abstract*—This study brings fundamental notions of the General Data Protection Law (LGPD) published in Brazil, its scope and the requirements that digital gaming companies will need to make, it also presents some relevant points on the construction of the Privacy Policy.**

***Index Terms*—LGPD, compliance, game business**

I. Introduction

In August 2018, Brazil published the Brazilian General Data Protection Law (LGPD - Law 13.709 / 2018) [1], and according to LGPD itself, it would come to force in August 14, 2020. This date has change several times but finally this law but at least a large part of its rules was enacted in 18 September 2020[1].

The LGPD was enacted in the same year as the General Data Protection Regulation (GDPR- Regulation 2016/679) [2] come to force and was greatly influenced by it.

The Brazilian law reflects the efforts of a worldwide trend to create a legal security scenario for the treatment of individual's personal data, including when it involves aspects such as the extraterritorial reach of companies and the data transfer.

Personal data protection laws do not seek to become an obstacle for developers[2] in the gaming industry. Instead, these standards allow for the safe and adequate data flow, observing the well-being of the consumer and the development of businesses, especial those of a technological signature or data-based nature.

In this sense, digital game developers need to be aware of legislative changes that directly or indirectly impact their activities, they need to understand the necessary procedures for adaptation and organize themselves in the best possible way. With LGPD, even though developers hire specialized services to carry out the compliance[3] process, when they need to understand how the data protection law reflects on their enterprise.

Using the qualitative and bibliographic research methods, this paper will seek to present the most sensitive points of the LGPD to assist companies in the compliance process for the creation of the Privacy Policy (and Cookie Policy), seeking to help companies in video game industry (such as developers, publishers and others) to understand what they will need to do for LGPD compliance.

This research will be presented as follows. Section one has the introduction and section two is about the importance of creating a culture of data protection will be addressed. In the third, the presentation of some existing regulations at the international level and guidance on which should be adopted for compliance. Section four will go into the study of the adequacy of the gaming company to Brazil´s General Data Protection Law, presenting sensitive points of Brazilian law that must be present in the company's data protection procedures, dealing finally with security and risk prevention and the national data protection authority.

II. Compliance among a plurality of laws

It is common for companies that develop digital games to overcome territorial barriers and market their products or services around the world.

In practical terms it is impracticable, economically and structurally, for small, medium and large enterprises in the gaming industry to comply with all privacy and personal data protection laws throughout the world.

Just for example, in European Union there is the GDPR which, together with other complementary directives, is applicable to the processing of personal data of all European citizens but each country can edit a supplementary standard, as is the case in Germany with the Bundesdatenschutzgesetz BDSG-New[4] and the Data Protection Act in Ireland[5].

In the United States, in the absence of a national law, state regulations are used, adopting territorial competence criteria

[1]The law n. 14.058/2020 was signed by President at September 17, 2020 and its effects start a day after, September 18. The penalties remain in effect only for August 2021, according to law n. 10.010/2020.

[2]For purely academic reasons, in this study the term "developer" will be adopted as a synonym for companies or single person who develops digital games, regardless of the Brazilian corporate modality.

[3]In Brazil has been common to hire companies specialized in carrying out assessments to define the adequacy levels of a company in relation to the LGPD and the accomplishment of data protection compliance, with a complete action plan for the company's compliance with the law. They range from sizable companies with branches across the country to small enterprises and law firms dedicated to compliance or "DPO (Data Protection Officer) as a service".

[4]To consult the BDSG-New regulation, visit: https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html#p0013. Access on: Aug. 1, 2020.

[5]The full text of the Data Protection Act is available in: https://dbei.gov.ie/en/Data-Protection/#. Access on: Aug. 1, 2020

such as the CCPA[6] (The California Consumer Privacy Act) in the State of California, or specialty of the subject, such as COPPA[7] (Children´s Online Privacy Protection Rule) aimed at protecting children and adolescents in the virtual environment. In a succinct way, these laws require parental consent for data processing of children under 13 (COPPA) and create new rights for consumers, giving them more control over their personal information.

Due to variety of laws in various countries or territories that regulate the topic of privacy and data protection, how should a developer of digital games be guided to achieve legal compliance, once them sell its virtual assets worldwide?

According to Boyd *et al*, "the ideal answer is to perform a rationalized compliance", in which it will be taking into account who the players are, where they are located, where the offices are and which countries have a stricter system privacy, especially in relation to foreign companies [3]. This will assist the company in deciding which adjustment to make.

Additional to the legislation, other rules and guidelines can serve as a guide for better adapting the company to data protection laws and the elaboration of privacy and cookie policies. Therefore, one must take into account the customs and good practices of the industry and self-regulatory systems, such as ESBR[8], PEGI[9] and that adopted by the *Ministério da Justiça* (Ministry of Justice)[10] for games marketed in the country.

As a result, the information provided in this study regarding Brazilian legislation seeks provide support to companies to achieve the best levels of adequacy.

III. Data Protection Culture

In the early 2000s, talking about company privacy was a simple task of creating and writing a privacy policy, but today it concerns an ongoing process within an organizational structure that involves analysis of computational and software structures, employees, relationship with consumers, commitment of financial resources and, still, specialized labor in compliance [3].

Privacy, Protection of Personal Data and Data Security are three distinct notions, although closely related to create a culture of protection within the company and facilitate compliance processes.

Privacy concerns about the feeling of security, subjective and individual, when, for example, it refers to a given treatment of the data of players, employees and third parties in accordance with the applicable legislation [3].

"*Privacy is the right to control the information about yourself (Nissenbaun), despite some cases which the law don´t ask for consent*".[4]

The Protection of Personal Data is based on objective criteria foreseen within a normative system. In Brazil, this system includes, in addition to the LGPD, the *Constituição Federal*[11] (Federal Constitution) that places the right to privacy as fundamental and other sectoral laws, such as the *Marco Civil da Internet* (MCI)[12] (Internet's Civil Framework) which already enshrines the protection of personal data, the consumer law *Código de Defesa do Consumidor* (CDC)[13] (The Consumer Law), the *Estatuto da Criança e do Adolescente* (ECA)[14] (Child and Adolescent Statute), law focused on child and teenagers protection, the labor law in *Consolidação das Leis do Trabalho* (CLT) (Consolidation of Labor Laws) and the *Código Civil* (CC) (Civil Code). All of these laws form a system that provides support for the LGPD.

Data Security combines both, the idea of security and privacy and consists of the adoption of concrete, administrative and technological measures to prevent unwanted access, either to the personal data of those related to the developer, or to information related to business secrets, such as contracts and the source code [5].

These measures may consist of using encryption and means of tracing company files, firewall technologies, physical security in the server room (such as locks, cameras, etc.), conducting internal audits frequently to monitor compliance, implementing a culture of password security on the developer's computers, among others.

The three elements together, help to create a culture of security and privacy within the gaming company, which go far beyond legal compliance with the LGPD: the collective understanding of the importance of personal data aligns different sectors of the company and improves adherence to the policy of privacy, generating a gain for all [6].

IV. Brazilian Data Protection Law for Gaming Businesses

The LGPD is a multi-sectoral law applicable to any operation and, mainly, to the collection of personal data carried

[6]The CCPA can be accessed through the link: https://oag.ca.gov/privacy/ccpa. Access on: Aug. 1, 2020.

[7]COPPA can be consulted through the link: https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule. Access on: August 1, 2020.

[8]ESRB (Entertainment Software Rating Board) is a private non-profit organization that establishes age rating for games marketed in North America, as a way to help consumers to choose.

[9]PEGI (Pan European Game Information), developed by the Interactive Software Federation of Europe in 2003, is a system for classifying games in the European Union.

[10]*Portaria do Ministério da Justiça* no. 1.189 / 2018, regulation which made this public entity responsible for creating the indicative classification for audiovisual works, including physical or electronic games. The last guidance was published in 2018 and can be accessed through the link: https://www.justica.gov.br/seus-direitos/classificacao/guia-pratico/classind-guia-pratico-de-udiovisual-3o-ed.pdf. Access: Jul. 31, 2020.

[11]It´s important to say that all brazilian´s laws are available only in Portuguese language at the official government website, but there is an English version of *Constituição da República*. Available on: http://www.stf.jus.br/repositorio/cms/portalStfInternacional/portalStfSobreCorte_pt_br/anexo/BrazilFederalConstitution_atualizadaataemenda99de2017Eletrni.._.pdf. Access in: Jul. 31, 2020.

[12]MCI - Law 12.965/14, available in: http://www.planalto.gov.br/ccivil_03/_ato2011-014/2014/lei/l12965.htm. Access in: Jul. 31, 2020

[13]CDC - Law 8.078/90. Avaliable in: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm.Accessin:Jul.31,2020.

[14]ECA - Law 8.069/90 avaliable in: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm.AccessinJul.31,2020.

in Brazil, even if the holder is located inside or outside the country [6].

According to LGPD (article n. 33) [1], it will be possible to transfer personal data to other countries, even those which do not have an adequate level of data protection, based on the specific and express consent of the data subject.

This protection law covers principles, definitions, legal bases for processing personal data, structuring of the national data protection system and penalties. The most sensitive points for a game business will be brought up next.

A. The compliance in the game business

For the company starting the process of adapting to the LGPD, it is important to form a multidisciplinary team committed to this task, which will take a few months to complete[15]. It is not a task that falls solely to the legal or to the Information Technology (IT) sector, it must involve the entire business structure to capture the concerns of each sector and understand how to capture all of them in a document that can cover the entire company.

BOYD *et al* [3] cites IT, Human Resources, Marketing and Legal as strategic areas for integrating this group to collect the data processed by the company, classify them, apply the bases and build the rules that will guide the company to adopt measures involving data protection. What is really important is the company´s commitment to compliance to make the perfect implementation.

The first step is to collect or understand this information already collected, which can be done through mapping, inventory or even through a document similar to the DPIA (Data Protection Impact Assessment) provided for in the GDPR[16][7].

In the LGPD, this document is grounded for in the article 5th, XVII, and article 38 and receives the name "*Relatório de Impacto à Proteção dos dados pessoais* – RIPD" (Report of Impacts for Protection Personal Data). According to the "*Guia de Boas Práticas da LGPD*"[8], a guidance create by Brazilian government, it is a fundamental document that demonstrates how personal data are collected, processed, used and shared and what are the measures to mitigate risks, in case of possible damages.

This report of impacts, in essence, like the DPIA, a document that proves compliance and should be seen as an instrument to support decisions that are taken in relation to the processing of personal data and therefore, although it is not mandatory in Brazil, it is important that it is done when needed.

Also, this report is not required by law as an essential document for implementing data security and privacy measures. What the law says is the ANPD (Brazilian Data Protection Authority) will be able to request it. However doing the data mapping and understanding its flows, life cycle and critical risks, build the report is a natural way to record all these processes that will, in the future, justify the Privacy Policy (and the Cookie Policy).

Whether with the DPIA report or with another chosen means, the scope is to carry out the data inventory of the company's data to assess the application of the principles, the data collection and the data life cycle[17] required by law and how the disposal will be done. The Data Classification is then used to understand how to protect information and, from there, build a Privacy Policy that meets the needs of the gaming company.

It´s important to note that Brazilian data protection law has a certain opacity about cookies which is why general treatment rules are applied in this case. This means in order to processes data collected from cookies, it must have the consent of the data subject. This consent can be made through a cookie wall with an opt-in structure, just like the Privacy Policy, which means that the data subject can agree or not to process his/her personal data and if he/she refuses, they´ll still be able to access the website.

The data can be classified by sector, by the need for applied confidentiality, what is sensitive data, data from children under 18, what data needs to be reported to public authorities, so forth.

They can also be organized based on the purposes of processing personal data (to generate charges, to register players and employees, to provide access levels to those who develop the game, etc.), explaining, from there, what are the necessary and adequate data collected for this purpose, the types of data, the legal bases and the form of collection.

This is, even, the most logical procedure, as seen by the author, especially when it is necessary to build a Privacy Policy in due of material or formal competence of each data protection law.

Also, the information in this paper intend to bring some important aspects from LGPD not only to provide a legal back up to apply this law in the company but also to support the Privacy Policy.

To better understand the steps in this process, the explanation is provided below.

B. Principles of Necessity, Adequacy and Purpose

There are several principles that should be taken into account when processing personal data like purpose limitation, accountability, security, transparency, that must be observed for the processing of personal data of Brazilians. All these principles can be found in article 6th of LGPD.

There are also sensitive personal data, like bio-metrics, sexual orientation and any visual record of the data holder (such as photo or footage).

[15]BOYD *et al* (2018) makes a projection of at least four months for a small company to be properly adapted to the data protection system of a country or region. In fact, it demands a lot of hard work of all subjects involved in the company business.

[16]GDPR does not clearly define what this assessment is, so the specifications are based on WP (Working Part) 248, April 2017. Available on: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.AccessonAugust4,2020.

[17]Data life cycle refers to: collection, archiving, processing (for classification, use, reproduction, evaluation, etc.), sharing and disposal. This is what it says the "*Guia de Boas Práticas – Lei Geral de Proteção de Dados (LGPD)*", a small guidance developed by the Brazilian government.

The processing of personal data must respect the purpose, that is, a legitimate, explicit and specific purpose informed to the owner. It must be used to achieve a specific objective, suitable for the purposes informed to the holder and according to the context of the treatment.

There should also be a note to justify the need for this data, and what it is intended to achieve, as the processing of personal data should be limited to the minimum necessary to achieve the purposes.

There are also the principles of free access to data by the data subject, transparency and data quality, security, damage prevention, non-discrimination and accountability and expenses report. Many of these correspond to the owner's rights.

C. Processing of personal data

The law adopts a broad definition of personal data far beyond the set of information that identifies people directly or indirectly, such as name, CPF (*Cadastro de Pessoa Física*, a type of individual registration number), or address. For LGPD, personal data is also considered to be what identifies holders remotely or indirectly, such as IP addresses, geolocation data, or even inferences of data from an identified natural person, according to art. 12, §2 of the LGPD (profiling).

At article 6th in LGPD, data processing consists of any collection, production, reception, classification, use, access, transmission, distribution, processing, filing, transfer, etc. operation. For all these actions, it must be observed the LGPD for processing personal data in Brazil.

Also, LGPD brings a large list of subject rights which reflects in personal data management. So, the data subject owner has the right to know about data treatment, about anonimization, request access or data deletion [9]. The specific procedures to exercise this right will depend on a specific regulation, which still doesn´t exist.

D. Legal bases to processing personal data in LGPD

Talking about the legal basis for data processing, according to Brazilian law, means justifying the legal basis for the processing of personal data[18] and for that, the gaming company must make a survey of all data that are treated by the company, maintaining those that comply with the principle of purpose, adequacy and necessity.

Within the environment of the digital game developer, personal data[19] can be viewed from essentially three perspectives: from the players of players (consumers); employees, service providers and third parties. The study will focus on the first two.

Player data is collected directly or indirectly, whether through game distribution platforms, browsers, linking profiles on social networks, among others. These data are collected, with informed consent (art. 7, I and art. 14 of LGPD), for the creation of behavior profiling, to provide targeted advertising, to track behaviors and ascertain unauthorized practices, such as hacking [10], or to improve products or services developed by the company.

All those who provide services, directly or indirectly, to the game business, are in the employees category or service providers, such as outsourced workers[20]. The LGPD does not refer directly to employees, but this law must be interpreted together with Protection of worker´s personal data from International Labor Office (ILO), 1997 [11].

The data of these providers may be collected, without consent, for various reasons, such as the obligation of legal duties such as federal taxes related to workers payment (art. 7, II) and for the execution of a preliminary contract or contracts, such as the service provision contract with the players and the employment contract (art. 7, V). If employees or service providers are minors, the consent of the legal guardian must be obtained.

The ILO recommendation says, for example, that the workers' right to privacy is unenforceable and that, therefore, in the case of monitoring within the company, employees must be informed of the legitimate reasons for the monitoring, schedule and techniques, and it should be applied to less intrusive.

E. Three data segments for LGPD

In LGPD there are three types of data: personal data (art. 5, I), sensitive personal data (art. 5, II and art. 11, I) and personal data of children and adolescents (art. 14).

Personal data is that attributed to a natural, identified or identifiable person and it may require consent in some cases but also may not (art. 7º and 9º).

According to the law, sensitive personal data usually require consent in any situation and are those, among others, relating to racial or ethnic origin, sexual life, political opinion or religious belief.

This data is hardly necessary for the supply of products and services involving digital games[21], but in this context, if necessary, they must observe the consent of the holder. Otherwise, in a game company sensible data may be required without consent, like bio-metric or photo information, as security measures to access the company or company systems.

This consent must be informed, unambiguous, non-generic and unambiguous: the holder must know exactly what he is authorizing (art. 5, XII), providing in the privacy policy, far beyond the combination of transparency and choice, more

[18]This idea came from GDPR, articles 5-10

[19]Considering the scope of the article is a company that handles non-sensitive personal data, the explanation will take into account the general rule. However, if the gaming company processes sensitive personal data, it must comply with the legal bases from article 11 of LGPD.

[20]Within the micro system that involves a large gaming company, there are employees hired under the CLT regime, specific sponsorship contracts or outsourced services provided by specialist companies, which will be governed by the *Código Civil*(CC) [Civil Code], as a rule. They range from developers, programmers, artists, engineers, receptionists, to streamers and e-sports professionals.

[21]However, there may be exceptions. Examples are gamified applications that regulate well-being or health, such as the MySugr application. Available on: https://www.mysugr.com/en/. Accessed on: August 4, 2020

effective instruments such as option to engage or disengage through the "opt in" system[22][4].

The personal data of children and adolescents is peculiar to the Brazilian data protection Law. This point is especially important considering the Brazilian public who consume digital games. According to the 2020 *BGS Data Folha* survey [12], 15

The processing of these data may or may not be sensitive data, but regardless, to carry out any processing operation, prior consent from parents or legal guardians, as a rule, will be required. For ECA, a specific Brazilian law for children and teenagers, the definition of children in this context is a person between 0 and 12 yeas old and teenager, 12 to 18 years old. The LGPD inserts, in the same category, all minors under 18, without making any distinctions such as those present in COPPA, which requires consent only for minors under 13.

The law requires that the consent of the legal guardian for the processing of data of children under 18 must be given in a specific and prominent way. It is a vague requirement and being one of the most sensitive parts of personal data protection compliance, Boyd [3] suggest that developers use another way to collect game experience data than by collecting personal data, at least until the account is verified by the legal guardian.

This verification can be done in several ways, but the authors recommend two: requesting an additional email to access the game, from the legal guardian, in which the developer will send information about the game, link to the privacy policy for the part clicking "opt in" and also a second form of confirmation, such as providing the credit card. Obviously, these measures depend on a previous step, that of the minor declaring, in good faith, his real age.[3]

Another important point is the treatment of this personal data for marketing and advertising purposes. For the purposes of advertising digital games or carried out within them, by the CDC it must be objective and not mislead the consumer (art. 6, IV and art. 36).

Advertising aimed at children, up to 12 (twelve) years old[23], using sound or visual resources with childlike appeal, with an interest in persuading them from consuming products, is abusive according to Resolution no. 163/14 of the *Conselho Nacional dos Direitos da Criança e do Adolescente* (CONANDA), a national council which inspect rights for children and adolescents.

These are issues in which the LGPD differs from other regulations and needs to receive special attention from game developers or publishers who intend to processing personal data in Brazil.

[22]Nissenbaun [10] points a problem in what she calls "transparency paradox". The consent has to be informed by knowing all the relevant information about collecting, processing, flowing and purpose but if the Privacy Policy is too much detailed it will be unlikely that a common person will read and understand but otherwise, summarizing those practices drains important details which can make an important difference. It is necessary to achieve a balance.

[23]The child's age is established in the *Estatuto da Criança e do Adolescente* (ECA) [Child and Adolescent Statute].

F. Data subjects

Also, LGPD has three types of responsible data subjects similar do GDPR. The data controller ("*controlador*"), natural or legal person which are responsible to determines the purposes about processing personal data (articles no. 37 until 41 of LGPD). The data processor ("*operador*") is the entity that performs the data processing on the controller´s behalf.

The DPO, Data Processor Officer ("*encarregado*", according to LGPD) is a natural person responsible to guide the company, their employees, solve the claims of data subjects and send data breach notification to Brazilian authority. The identity and ways of contact to DPO must be public and clear for all the data subjects.

G. Data breach incidents

This represents a very important issue to mention on the Privacy Policy. The company needs to adopt means to guarantee the security of the data processing and plan the measures that will be taken in case of any security breach.

That is why gaming companies must take measures to ensure privacy, protection of personal data and data security, under the terms mentioned above. This implies reviewing the entire information security structure, using encryption techniques during the transfer of this data, managing data deletion, updating software, cookie policy, educating employees to create more secure passwords, constantly verifying levels of access and, also, the elaboration of a plan to respond to personal data security incidents.

According to LGPD (art. 46), security incident consists of any unauthorized access to such data or accidental or unlawful situations that generate loss, destruction, alteration or any form of improper or unlawful treatment. In the event of a security incident that may generate significant risk or damage to the holders, the controller must communicate to the data protection authority ANPD (*Autoridade Nacional de Proteção de Dados*) and, if possible, already adopt the necessary measures to reverse or mitigate these damages.

H. Civil liability for processing personal data

In Brazil there is disagreement about the nature of data processing activity that will reflects in the civil liability. The most accepted theory, so far, is that the activity of processing personal data is an activity with high risk and the law exists to reduce the risks of harm.

Thus, LGPD in articles 42 and 43 provides information about civil liability regardless of company fault (*responsabilidade civil objetiva*) in case of leak personal data unless the game company demonstrates that the fault is exclusive of the data subject, or that the company has not processing the data that cause damage to the data subject or, if the company proves that the data processing was carried out to the extent permitted by law.

It is important to remember that, by the art. 45, if during the processing of personal data occur any damage to the holder, the duty to repair with the possibility of applying the CDC

will arise when dealing with a consumer relationship, that is, between the gaming company and the player.

I. Brazilian Structure for Data Privacy

The LGPD determines the creation of the ANPD, which represents a national data protection authority. This important organ it will be responsible the construction of directives and good practices in data management in Brazil (art. 55-J). It is also responsible for the inspection and application of fines involving the irregular processing of personal data.

In Brazil, the authority has not yet been created, but there is an expectation that this will happen soon, given that the government has already taken the first steps to discuss the construction of this Authority.

While the ANPD does not exist, it does not mean that the LGPD is inapplicable. The law, coming into force when the ANPD is not yet constituted, will have its effects and may imply civil liability, depending on each case.

J. Another points about building a Privacy Policy

Privacy Policy is a document which the gaming company will inform their consumer player about processing personal data and has to be in accord with all Brazilians laws.

In the Privacy Policy, the gaming company should be clear about all the types of player monitoring to adopt anti-cheat measure and to make advertisement.

Also, the game company have to follow rules of International Standardization Organization (ISO) no. 27001, about manage methods of data security [13]; no. 27002 about good practices of management data security [14] and no. 27701 to manage privacy information and methods to prevent risks [15].

V. Is LGPD compliance really necessary?

Personal data represents a significant resource for several digital businesses and gaming industry isn´t left out, since the data-based economy corresponds to a primary market resource aimed at enhancing financial results.

One of the main points do compliance not only to LGPD but also to most of data protection regulations in the world is the Privacy Policy.

This document must represent the company´s internal data processing policy which is logically created after a deep understanding about data processed, data mapping, data flow, access levels, data cycle and another legal requirements.

If the game company intend to sell games in European Union (EU) it must comply with GDPR to process personal data from European citizens (even those outside Europe), people who lives in EU or companies based in EU (according to art. 3). If the personal data belongs to consumers living in California, regardless their nationality, CCPA will apply. If the personal data are processed in Brazil, regardless whether they are Brazilian, European or any other nationality, LGPD will be applied.

Formal and material competence is further complicated when it studied by the structure of many gaming companies: data is collected in one country, classified in another country and, finally, stored on servers located in a third country.

The solution to international conflicts of these rules is still under discussion and that´s why adopt a rationalized compliance is, for now, a safer way.

In theory, the Privacy Policy should be accessible to the data subject, contain clear and objective language, the name and contact of DPO and should, as far as possible and using rationalized compliance, respecting the countries laws on data processing. In practice, there are still doubts about which law to follow whether it will be necessary to create an specific policy for each country whether the company will need to have a DPO for each country and even, if the trade off resulting from this adaptation will find resistance from of game industry.

Even though LGPD was enacted in 2018 and entered into force on September 18th 2020, until the submission of this work, Just a few game companies in Brazil are compliant with data protection national law.

Wildlife for example has in its homepage the Privacy Policy [16] and Privacy Policy for Candidates for a Job [17], all already suitable with LGPD.

Hoplon has a Privacy Policy [17] on its website that´s only suitable with GDPR and United States Department of Commerce from USA. Companies like Aquiris, Kokku and Behold Studios, by the other hand, don´t have a Privacy Policy available in their website.

LGPD, like several data protection regulations, are forcing companies data-base business to rethink and reform their structure. These laws don´t prevent the personal data processing: they only limit and require more transparency by the companies.

This idea needs to be put in mind in the implementation of the privacy culture and of all the decisions that will be taken for compliance. After all, the cost of not adapting is reasonably high, since the fines for the irregularity compromise from 2

So far, data protection compliance is not an option for those companies that process personal data in Brazil and want to avoid bottlenecks in their activities.

VI. Conclusion

The Brazilian law that regulates the protection of personal data in Brazil is the LGPD, which has many similarities with the GDPR, which can facilitate its understanding for foreigners. Although not yet came into force, game companies that intend to maintain or start processing personal data of players in Brazil must understand the local adequacy process, even if they contact a specialized company to perform compliance.

For compliance and the implementation of a privacy policy within the gaming company to have positive results, it is important that an internal culture of protection is created and nurtured beforehand, engaging all sectors to understand how important it is to guarantee privacy, protection and the security of that information.

The adequacy process begins with the survey of the company's data, either by preparing a DPIA or by other mechanisms, such as the data inventory, understanding the processes of collection, storage, life cycle of this data and other important aspects. From that, the classification of these data begins,

which can be carried out based on criteria defined by the company itself, either from the type of data collected, or in relation to each sector of the company, or from the purpose.

In the process of collecting, classifying and constructing the policy, other points should also be taken into account, such as the principles brought up in the LGPD, the three data segments that vary from consent and the legal bases for processing personal data.

The data policy must also consider preventive mechanisms in terms of information security and have a containment plan.

ANPD is, by law, the authority responsible for creating directives and supervising the processes of processing personal data. Although the authority has not yet been structured in Brazil, it does not imply that personal data can be processed without observing by the LGPD.

Although, at first, it may present compliance costs, the company's adaptation to the General Data Protection Law creates opportunities that can elevate business to a higher level of confidence in relation to consumers and providers, in addition to adding in terms of competitiveness and reputation.

REFERENCES

[1] Brasil. Lei Geral de Proteção de Dados Pessoais (LGPD). 14 de agosto de 2018. Avaliable in: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Access: Aug 1st, 2020.

[2] European Union. General Data Protection Regulation. 2018. Avaliable in: https://gdpr-info.eu/. Access in: 14 ago, 2020.

[3] G. Boyd; S. F. Kane; B. Pyne. ".Video Game Law: everything you need to know about legal and business issues in the Game Industry". CRC Press: Boca Raton. 2018.

[4] H. Nissenbaum. "A Contextual Approach to Privacy Online" in Daedalus - Journal of the American Academy of Arts Sciences. 2011.

[5] A. Weller; E. Leach. "How to build a 'culture of privacy'". IAPP. Feb, 2020. Avaliable: https://iapp.org/news/a/how-to-build-a-culture-of-privacy/. Access: Access: Jul. 30, 2020.

[6] R. Leite Monteiro. "The new Brazilian General Data Protection Law – a detalied analysis". IAPP. Aug, 2018. Avaliable: https://iapp.org/news/a/the-new-brazilian-general-data-protection-law-a-detailed-analysis/. Access: Aug 1st, 2020.

[7] European Union. WP 248. Apr, 2017. Avaliable: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236. Access: Aug 4th, 2020.

[8] Governo Federal. "Guia de Boas Práticas – Lei Geral de Proteção de Dados (LGPD)". Apr, 2020.

[9] A. Frazão; M. Donato Oliva; V. da Silveira Abilio. "Compliance de dados pessoais" in A Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro. 2019. Thomson Reuters Revista dos Tribunais. São Paulo.

[10] K. Orland. "Ring 0 of fire: Does Riot Games´ new anti-cheat measure go too far?". in Ars Technica. 2020. Avaliable in: https://arstechnica.com/gaming/2020/04/ring-0-of-fire-does-riot-games-new-anti-cheat-measure-go-too-far/. Access: Jul. 30, 2020.

[11] ILO. Protection of workers. personal data.1997. Avaliable in: https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf. Access: Jul. 31, 2020.

[12] BGS/ Data Folha Survey 2020. Avaliable: https://www.brasilgameshow.com.br/estudo-mercado-de-games/. Access: July 30, 2020.

[13] ISO/IEC n. 27001. "Information Security Management". 2013. Avaliable: https://www.iso.org/standard/54534.html. Access: Jul. 30, 2020.

[14] ISO/IEC n. 27002. "Information technology – Security Techniques – Code of Pratice for information security controls". 2013. Avaliable: https://www.iso.org/standard/54533.html. Access: July 30, 2020.

[15] ISO/IEC n. 27701. "Security techniques – Extension to ISO/IEC 27001 and ISSO/IEC 27002 for privacy information management – Requires and guidelines". 2019. Avaliable: https://www.iso.org/standard/71670.html. Access: July 30, 2020.

[16] WilfLife. Política de Privacidade. Jul, 2020. Avaliable in: https://wildlifestudios.com/pt-br/politica-de-privacidade/. Access: 20 sep, 2020.

[17] WildLife. Política de Privacidade de Candidatos. Jul, 2020. Avaliable: https://wildlifestudios.com/pt-br/politica-de-privacidade-de-candidatos/. Access: 20 sep. 2020.

[18] Hoplon. Política de Privacidade. Ago, 2017. Avaliable in: http://www.hoplon.com/site/privacy-policies.php. Access in: 20 sep, 2020.