THE EU GENERAL DATA PROTECTION REGULATION AND THE BRAZILIAN COMPANY

BAPTISTA LUZ
ADVOGADOS

/ THE IMPACT OF THE EUROPEAN GENERAL DATA PROTECTION REGULATION ON BRAZILIAN COMPANIES

Global Reach and International Data Transfer

Renato Leite Monteiro

With this study we will look into the possible impacts of the new European Regulation on Brazilian companies as of 2018. The idea is to address the main impacts, i.e. changes, as well as to understand what is applicable in accordance with the level of interaction between Brazilian and European companies. Among the points we will deal with we have included whether applicability/impact is the same for European subjects' data which are stored/processed in Brazil.

Nevertheless, before getting into the new obligations of the controller of personal data we shall show the scope of application for such Regulation, the conditions that allow the international transfer of data, its extra-territorial reach and how the Personal Data Protection Authority can enforce the Regulation upon companies that are not located within the European Union, and thus verify whether the Regulation applies to Brazilian companies.

A crucial point worth of attention in the first place is **that the GDPR applies to the gathering of personal data belonging to natural persons within the European Union regardless of nationality, citizenship, domicile or residence.**

Furthermore, with this study we will see if Brazilian companies, in any way gathering, processing or receiving personal data of natural persons located in the European Union regardless of their nationality, including data related to consumers, collaborators, finance, or services provided to any of the 28 countries of the European Union, may be subject to the jurisdiction prescribed by the norm and compliance would have to impact their operations and transaction costs.

The fines established in the GDPR notwithstanding, a Brazilian company can only contract companies that are also in conformity, even if it does not directly have the elements and/or contact points for the application of the new regulation, in case it provides data processing services to other companies, such as gathering, storing, enrichment, profiling, and it is contracted or subcontracted by companies subject to the GDPR. The new legal obligation may occasionally be the cause for justified contract termination with no right to contractual fines and penal clauses in case such premise is not provided for in the agreements.

/ EXECUTIVE SUMMARY - EXTRATERRITORIAL REACH

/ Extraterritorial application - reaching Brazilian companies with branches in the European Union or providing services in the European market.

/ applies to companies with a branch or representative in the European Union.

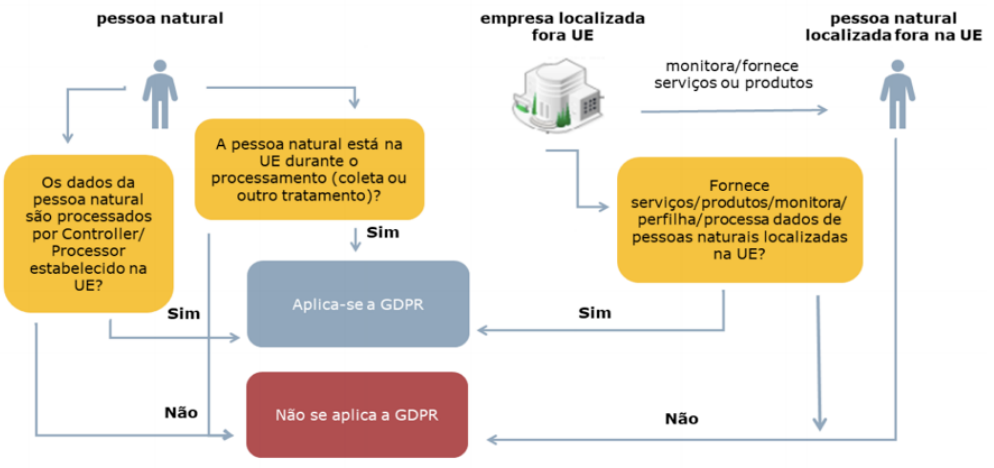
/ applies to companies providing services to the European market even if not physically located in the EU.

/ applies to companies gathering data of subjects in the European Union regardless of nationality, even if not physically located in the EU.

/ applies to companies outsourcing data processing for companies located in the European Union, even if not physically located in the EU.

/ Suppliers (date processors) obligation of conformity -> cause for contract termination
/ Fines in amounts up to 20 million euros or 4% of global revenue.

/ CHART - EXTRATERRITORIAL REACH



/ WHAT IS GENERAL DATA PROTECTION REGULATON - GDPR

The General Data Protection Regulation (EU Regulation 2016/679[1] was adopted by the European Union in April 2016 in order to substitute Directive 95/46/EC (the "Directive") known as European Directive for Personal Data Protection. The main purpose of the GDPR is to update, modernize and harmonize the legal structure of personal data protection in the European Union, granting individuals more control over their data

[1] http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

while fostering the economic and technological development as well as innovation. The Regulation[2] was under vacation legis and should come into force as from May 25, 2018, effectively substituting the Directive in question. The Regulation will have a global effect, since it applies to entities processing personal data, even beyond the borders of the EU insofar as goods or services are provided to data subjects located within the European Union or in case the behavior of those data subjects located in the EU is monitored.

/ CONCEPT OF PERSONAL DATA AND DATA PROCESSING

The scope of the application of the norms for personal data protection is intrinsically connected to what can be considered personal data. The Regulation adopts, in its Article 4, an expansionist concept[3], going beyond the data that effectively identifies a natural person, so as to also include the concept of identifiable as long as the steps taken for identification through data crossing-adding-combining are not unproportionate. Thus, what follows is personal data in the concept of the Regulation:

> "any information related to a natural person identified or identifiable. A natural person that is identifiable is someone who can be identified, directly or indirectly, mainly through a reference to a unique identifier, such as name, identification number, location data, electronic identifier or one or more factors specific to physical, physiological, genetic, mental, economic, cultural or social identity of the natural person"[4]

The Regulation also adopts, for profiling purposes, a consequentialist concept[5] of data which can occasionally determine that data not strictly under the concept of personal data as provided for in Art. 4 may be covered for purposes of application of the norm, such as anonymized or pseudo-anonymized data[6].
Moreover, in order to determine the practices that are subject to the rules set forth by the Regulation, it is necessary to keep in mind that its concept of processing is as follows:

---

[2] Regulation that, unlike Directives, has an immediate application on all members of the European Union without the need of internalization through a national norm. Thus, the rules established in the Regulation, with some exceptions, are uniform for all 28 members.

[3] BIONI, Bruno. Xeque-Mate: the triplet of personal data protection in the game of chess of the legal initiatives in Brazil. Study Group on Public Policy when Accessing Information of USP-GPOPAL.

[4] Art. 4 (1) "personal data" means any information relating to an identified or identifiable natural person ("data subject") and identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; (literal translation)

[5] Op. Cit. 3.

[6] Opinion 05/2014 on Anonymization Techniques of Article 29 Working Party, Available at: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216en.pdf

"Any operation or group of operations conducted on personal data or packs of personal data through automatization or not, such as cataloging, recording, organizing, structuring, storing, adapting or modifying, gathering, consulting, use, broadcasting, publication or any other means that make them available, aligned, combined, restricted, deleted or destroyed[7]"

To sum it up, insofar as it is under its jurisdiction, the Regulation subjects any personal data processing practice to its own rules, limits, obligations, granting data owners a series of rights, most of which not provided for in the Directive of 1995.

/ INTERNATIONAL DATA TRANSFER

The Regulation allows the transfer of person data to third-party countries away from the European Union through a series of conditions, insofar as the European Union considers it a country with an adequate level of personal data protection, which is not the case of Brazil[8]. Art. 45[9] sets forth the conditions for the international transfer based on decisions of adequation, which regard to a country as having an adequate level of protection. Considerando 104[10] specifies what decisions of adequacy are granted to countries with a level of protection similar to such guaranteed in the Union.

Despite the lack of a decision by the Commission, considering the country as adequate, transfers are also allowed to countries away from the

---

[7]

[8] In South America, only Argentina and Uruguay have received the seal for an adequate level.

[9] Art. 45 91) "A transfer of personal data to a third country or an international organization may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organization in question ensures an adequate level of protection. Such a transfer shall not require any specific authorization."

[10] Considerando 10 - Criteria for an adequacy decision: In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country or of a territory or specified sector within a third country, take into account how a particular third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defense and national security as well as public order and criminal law. The adoption of an adequacy decision with regard to a territory or a specified sector in a third country should take into account clear and objective criteria, such as specific processing activities and the scope of applicable legal standards and legislation in force in the third country. The third country should offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union, in particular where personal data are processed in one or several specific sectors. In particular, the third country should endure effective independent data protection supervision and should provide for cooperation mechanisms with the Member States' data protection authorities, and the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress."

European Union under some circumstances[11], such as the use of standard contractual clauses - generic clauses previously approved by the European Commission before being introduced in the contracts regarding international transfers - or Binding Corporate Rules (BCR)[12] approved by the domestic authorities protecting personal data in particular cases, such as a company or a specific economic group[13]. In both situations, the process is considered severely bureaucratic, mainly due to the fact of removing the simple autonomy of the parties in order to establish the protection standards, since the intervention of the state in what is to be decided is obligatory.

Moreover, the Regulation innovates when introducing, in its Art 42[14], the possibility of authorizing the transfer to third countries through seals,

[11] Art. 46 (1) (2): In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organization only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorization from a supervisory authority, by:
- a legally binding and enforceable instrument between public authorities or bodies;
- binding corporate rules in accordance with Article 47;
- standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);
-standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);
- an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
- an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

[12] Art. 47 (1) "The competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 63, provided that they:
- are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;
- expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and fulfil the requirements laid down in paragraph 2.

[13] Considerando 110 - Binding corporate rules: A group of undertakings, or a group of enterprises engaged in a joint economic activity, should be able to make use of approved binding corporate rules for its international transfers from the Union to organizations within the same group of undertakings, or group of enterprises engaged in a joint economic activity, provided that such corporate rules include all essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.

[14] Art. 42 ((1) (2): Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.

certificates, as long as binding and applicable legal instruments are agreed upon with the entity responsible for processing the data looking to guarantee the proper protections.

/ INTERNATIONAL TRANSFERS BASED ON LEGAL INSTRUMENTS

The Regulation also lists other instruments which authorize the international transfer of data[15] insofar as the processing of personal data is based on legitimate processing with express consent or similar duty. As follows:

- The data subject has expressly authorized the international transfer of their data after being informed of the possible risks of such transfer due to the absence of an adequacy decision and appropriate safeguards[16].

It is important to point out that in regard to the international transfer of data, the Regulation requires explicit consent instead of unequivocal consent. Pursuant to the Regulation, unequivocal consent allows the data subject to inform their desire to authorize the processing of their data through a declaration or an affirmative action, such as behavior[17], Explicit consent, on the other hand, requires that the data subject reply actively to a question, verbally or in writing, as defined by Article 29 Working Party[18].

Pursuant to Art. 13[19] of the Regulation, the entities responsible for the processing of data shall provide certain information to the data subjects upon obtaining their explicit consents, such include:

In addition to adherence by controllers or processors subject to this Regulation, data protection certification mechanisms, seals or marks approved pursuant to paragraph 5 of this Article may be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation pursuant to Article 3 within the framework of personal data transfers to third countries or international organizations under the terms referred to in point (f) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including with regard to the rights of data subjects".

[15] Art. 49 (1).

[16] Art. 49 (1) (a): "the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards";

[17] Article 4 (11)

[18] Opinion 15/2011 on the definition of consent of Article 29 Working Party: "respond actively to the question verbally or in writing". Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf

[19] Art. 13(1): Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time the personal data are obtained, provide the data subject with all of the following information:
- the identity and the contact details of the controller and, where applicable, of the controller's representative;
- the contact details of the data protection officer, where applicable;

- The entity responsible intends to transfer their personal data to a third country outside of the European Union;
- That such transfer be made to a country which obtained an adequacy decision of a protection level for personal data; or
- Reference to the adequate or appropriate safeguards to guarantee their rights and how to obtain them.
- Such information must be provided concisely, with transparency, intelligibly and easy to access, in a simple and clear language, pursuant to Art.12[20].
-

Other possibilities of international transfer are:

- when the transfer is necessary for the execution of a contract between the person responsible for processing and the data subject, or for the implementation of precontractual measures, required by the data subject[21];
- when the transfer is necessary for the conclusion or execution of a contract in the interest of the data subject, but entered into by the person responsible for its processing and a third party, either natural or legal[22];
- when the transfer is necessary due to the underlying public interest[23].

An important innovation of the Regulation was the introduction of the possibility of international transfers to third countries or entities based on the legitimate interests of the person responsible for data processing in

---

- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
- the recipients or categories of recipients of the personal data, if any;
- where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

[20] Art. 12 (1): "The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication, under Articles 15 to 22 and 34 relating to processing, to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means".

[21] Art. 49(1)(b): "the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request";

[22] Art. 49(1)(c): "the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person";

[23] Art. 49 (1)(d): "the transfer is necessary for important reasons of public interest;

the event the cases above are nonexistent, including adequacy decisions, standard clauses or BCRs. This kind of transfer is possible insofar as:

- "it is not repetitive; it is limited to a restricted number of data subjects and is necessary to the legitimate interests of the person responsible for data processing without overriding the interests, rights and freedoms of the data subjects, and the person responsible for the processing has addressed all circumstances related to the transfer of the data in order to provide appropriate safeguards to the personal data"[24].

The case of international transfer based on legitimate interests is similar to the authorization case of data processing for other purposes, after the effective test of proportionality[25], nevertheless limited to a small group of data subjects, and limited to a few occasions.

/ EXTRATERRITORIAL REACH

Before any detailed analysis it is necessary to make the affirmation that the territorial efficaciousness of the Regulation does not lead, in any moment, to purposes of determination of jurisdiction or where and when the norm will be applied, the nationality of the data subjects as natural persons. **In other words, GDPR does not only apply to European citizens as nationality is not an element to consider.**

To corroborate this understanding, the European Counsel has recently published[26] a correction to the wording of Art. 3(2) of the Regulation, since its translation from the English language (original) led to some interpretation concerns which caused some misunderstanding that the GDPR would only apply to the data of subjects that are residents in the EU (without any mention at that point to nationality or citizenship). The "who are" concept in English was wrongly translated as "resident" into Portuguese, which is a legal concept, however, the lawmaker referred to natural persons located in territory within the 28 member countries of the EU. See comparisons below:

[24] Art. 49(1)(only paragraph): "not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data."

[25] Considerando 47: "The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller".

[26] Publication of the European Council with the corrections in several languages, including Portuguese: http://data.consilium.europa.eu/doc/document/ST-8088-2018-INIT/en/pdf

Previous Wording	Corrected Wording
"2. This regulation applies to the processing of personal data of subjects **residing** within the territory of the Union, made by a person responsible for the processing or subcontractor not established within the Union, whenever the processing activities are not related to:"	"2. This regulation applies to the processing of personal data of subjects **who are** within the territory of the Union, made by a person responsible for the processing or subcontractor not established within the Union, whenever the processing activities are not related to:"

Therefore, **the GDPR applies to the gathering or personal data or natural persons who are in the European Union, regardless of their nationality, citizenship, domicile or residency.**

To continue, the points of contact below are elementary marks to verify whether the GDPR applies to a company, whether it is physically located in the European Union or not. Below is a brief summary:

- Extraterritorial Application reaching Brazilian companies with branches in the European Union or which provide services in the European market;
- Applies: Company with a branch or representation in the European Union ("EU");
- Applies: Company, even without a physical presence in the EU, but which provides services in the European market;
- Applies: company, even without a physical presence in the EU, which gathers data of natural persons located in the EU, regardless of nationality;
- Applies: company, even without a physical presence in the EU, which monitors natural persons located in the EU, regardless of nationality;
- Applies: company, even without a physical presence in the EU, which outsources data processing for companies located in the EU.

The Regulation innovates in relation to the Directive drastically increasing the limits of its jurisdiction so as to also include those responsible for the

data processing who are geographically outside of the European Union. Thus, the Regulation must apply when:

- The data processor is geographically located in a member country of the European Union and has a principal place of business, irrespective of whether it is the headquarters or a subsidiary, or under legal basis. **The nationality of data subjects is irrelevant.** Under this case, the person responsible shall be subject only to the supervision of an authority of personal data protection of the place of the main establishment[27].

- If the data processor is geographically located outside of the European Union and provides services or products to residents in the European Union or monitors the behavior of residents in the European Union[28]. Under this scenario, not only shall the data processor be under the jurisdiction of the Regulation, but also be subject to the supervision of all personal data protection authorities of countries to which it provides services or products; or monitors the behavior of its residents.

However, the Regulation does not make it clear what would be services or products or monitoring behavior. Only that there should be an intention to provide services to a certain member country. To determine intent, the language used and the transaction currency can be taken into consideration. With regard to monitoring, such does not depend on a business relationship or payment, and it can go beyond online tracking, but the types of its practice and the technologies will still be the matter for discussion[29].

Another point left unclear by the Regulation in determining its jurisdiction is the concept of data subjects located in the European Union, regardless of nationality, since it does not define whether such subjects would be

[27] Art. 3(1): "This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not".

[28] Art. 3(2): "This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
- the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
- the monitoring of their behaviour as far as their behaviour takes place within the Union.

[29] Considerando 24 - Applicable to processors not established in the Union if data subjects within the Union are profiled: "The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes".

those who reside in the member countries or also those who are there but do not effectively reside. The best doctrine has understood that the mere physical location, even if temporary, of a natural person, irrespective of their nationality, in any of the 28 member countries of the European Union, or places in the world under its jurisdiction, would give rise to the extraterritorial reach[30].

As mentioned above, data processors who are outside of the European Union cannot avail themselves of the concept of one-stop-shop, that is, to respond to the data protection authority of only one country, even if they process data in reference to other member countries. In this scenario, the data Processor will be subject to the authorities of all countries and must appoint a representative before the authorities of each one, which can increase the operational costs.

The domestic authorities may take action against the representatives of those located in their territories, not against those responsible for the processing if they are in third countries. But these can order, for example, that operators of communication infrastructure, such as telephony companies, block access to the services provided by the person responsible. In both situations there is a very high reputational damage risk, which can influence the decision to cooperate with the authorities.

/ ENFORCEMENT - APPLICATION OF FINES AND CONTRACT TERMINATION

If, due to the contact points described above, a company is under the Regulation, and must therefore be in conformity with it, in the event it decides not to adequate, penalties may reach 20 million Euros or the 4% of the overall turnover of the company or its economic group, whichever amount is higher[31].

---

[30] MADGES, Robert. GDPR's global scope: the long story. Available at: https://medium.com/mydata/does-thegdpr-apply-in-the-us-c670702faf7f

[31] Art. 83(5). Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20,000,000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:
(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;
(b) the data subjects' rights pursuant to Articles 12 to 22;
(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;
(d) any obligations pursuant to Member State law adopted under Chapter IX;
(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).
Art. 83 (6). Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20,000,000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

However, if a company is not effectively located in the European Union, has not appointed any representative before the authorities[32], or appointed a Data Protection Officer (DPO)[33], any Data Protection Officer of any of the 28 Member States of the European Union may find it difficult to enforce penalties, due to which it may be necessary to use international cooperation instruments for this purpose, which at times can be extremely slow and bureaucratic.

Nevertheless, the Regulation expressly determines that the person responsible can only contract Operators who are in compliance with the GDPR[34]. Thus, the processor may, due to a new legal obligation effective as of May 25, 2018, have to terminate the processing contracts or outsourcing of any type of treatment of personal data, such as storage, enrichment, matching, consultation, profiling, with companies that are not aligned with the GDPR, even if they are in Brazil. This cause of termination may even be justified without any right to a fine or indemnity if this scenario is not provided for in the contract, as it is a law measure to which the Officer is obligated. Therefore, the Officers that are compliant will have a blue ocean[35], as contracting will only be possible with them, thus limiting the activity of a myriad of competitors. In other words, being in compliance with the GDPR can be considered a competitive edge.

[32] Art. 27(1). Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union.

[33] Art. 37(1) The controller and the processor shall designate a data protection officer in any case where:
(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
(b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
(c) the core activities of the controller or the processor consist of processing on a large scale of special
categories of data pursuant to Article 9 or personal data relating to criminal convictions and offences referred to in Article 10.

[34] Art. 28(1): Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

[35] It is a business concept introduced in a book of the same name, according to which the best form to overcome competition is to stop trying to overcome it, i.e. look for markets yet to explore to which the author of the concept referred as “blue ocean”. KIM, W. Chan. The Strategy of the Blue Ocean.

/ CONCLUSION

Based on the foregoing, **any Brazilian company may be subject to the jurisdiction prescribed by the Regulation if it gathers personal data of natural persons or legal entities located in the European Union or provides services and products directly in the market of the members of the European Union, and if it treats data of natural persons located in the economic block.** If this is the case, we recommend a deeper study of the rules, limitations and obligations imposed by the norm because of the duty of conformity.

In addition, Brazil is not considered by the European Commission as a country with an adequate level of data protection. Therefore, the transfer of personal data of subjects located in the European Union, directly or indirect, can only happen based on one of the hypotheses of authorization. For operational and bureaucratic reasons, we recommend the use of contractual clauses in which the subject located in one of the member states expressly authorizes, in accordance with the above information rules, the transfer of their personal data to Brazil or a country where the company will process such data, as in cases of outsourcing and cloud computing services.