Privacy Series

13 TEST YOUR KNOWLEDGE ABOUT THE LGPD

VEIRANO ADVOGADOS



This is the thirteenth chapter of the Data Privacy Series. Click here to access the chapter 12.



In 2023, the Brazilian General Data Protection Law (Law No. 13,709/2018 or "LGPD") celebrates 5 years of its publication - now also including the possibility of the application of administrative sanctions by the ANPD since August 2021. The Brazilian National Data Protection Authority ("ANPD") has been active in fostering discussions and disseminating concepts, practices and principles of privacy and data protection, through the publication of several materials for awareness and regulation of the LGPD since its creation.

Veirano Advogados has been following and participating in discussions regarding these issues. For this reason, our Data Protection & Privacy team has prepared the Privacy Series, in which we will periodically publish on different topics related to privacy, bringing not only LGPD concepts, but also ANPD publications on the subject, relevant considerations, among other contents.

INTRODUCTION

In Chapter 13 of the Privacy Series, we will test your knowledge of the LGPD, covering the main concepts of the law, as well as revisiting topics that have already been covered in previous editions of the Privacy Series.

For further information, check out the previous chapters of the Privacy Series:

Ed.1 | What to expect in 2023? – access here

Ed. 2 | Why should I be concerned with the LGPD? – access here

Ed. 3 | The Processing Agents – access here

Ed. 4 |Data Protection Officer ("Encarregado") – access here

Ed. 5 | Principles and the Processing of Personal Data – access here

Ed. 6 | Consent – access here

Ed. 7 | Legitimate Interest – access here

Ed. 8 | Rights of Data Subjects – access here

Ed. 9 | Administrative Sanctions – access here

Ed. 10 | International Data Transfer – access here

Ed. 11 | ANPD and its directives – access here

Ed. 12 | How do I ensure compliance? – access here



TEST

1. I want to send free gifts to my clients or news about my products. Do I necessarily need their consent to do so?



- ☐ a. Yes. Processing data for marketing purposes always requires the client's prior and informed consent.
- ☐ b. No. Sending gifts/news to clients is a promotional activity of the company, which does not require consent in all cases.
- ☐ c. No. In some cases, it is possible to base data processing for promotional purposes on legitimate interest.

2. I received a request for access to an individual client's data by e-mail. What should I do?



- ☐ a. Leave the request in my inbox and do nothing.
- ☐ b. Depending on the content of the data subject's (individual client) request, I respond immediately in a simplified format or within 15 days from the receipt of the request, by means of a clear and complete statement.
- ☐ c. I acknowledge receipt and send a form in response, requesting that the client provide me with other personal data, in addition to what I already have in my databases, to validate his/her identity.

3. Can I condition the user's registration to the inclusion of a profile photo on my platform?



- ☐ a. Yes, as long as the photo is necessary for provision of the services or for purposes of better identifying the data subject or if the data subject consents to processing.
- ☐ b. Yes, because the user's profile photo is an aesthetic requirement to improve the platform's dynamics.
- ☐ c. No. The profile photo is sensitive personal data; therefore, it cannot be a requirement for the user's registration on the platform.

4. My e-commerce company suffered a cyber attack, which caused a breach in my consumers' data, revealing the names, addresses and access passwords of more than 100 customers. Who should I notify?



- ☐ a. Only the data subjects involved in the data breach.
- ☐ b. Only the ANPD.
- ☐ c. The ANPD and the data subjects involved in the data breach.

5. A certain medical clinic buys a database on payments to HCPs ("HealthCare Professionals") for the purpose of organizing lectures on the health area. It happens that, when contacting one of the HCPs, the buyer (the medical clinic) receives a complaint from the data subject (HCP), who claims that he has not given consent to the processing of his personal data by the buyer. In this scenario, can the medical clinic be held responsible for the aforementioned breach of the personal data protection legislation?



- ☐ a. Yes. The buyer can be held jointly liable, because he is directly involved in the processing of data that resulted in damage to the data subject.
- ☐ b. No, because the buyer acquired the HCP database, trusting that the seller had obtained the consent of the data subjects.
- ☐ c. No, because the LGPD does not cover relationships of a civil nature, such as those inherent to purchase and sale contracts.

6. The role of the Data Protection Officer (DPO) is to function as a communication channel between the controller, the data subjects and the National Data Protection Authority (ANPD). Regarding the figure of the DPO, what are the requirements that you must fullfil for its appointment?



- [ ] a. The contact information of the DPO should be publicly disclosed in a clear and objective manner, preferably on the controller's website.
- [ ] b. The DPO must have legal and regulatory knowledge on the subject, and professional certifications on data protection (recommended but not mandatory).
- [ ] c. In addition to the contact information of the Officer in Charge, its identity should also be publicly disclosed in a clear and objective manner, preferably on the controller's website.

7. Which of the following is **CORRECT** regarding consent?



- [ ] a. Consent is only required for cases of sending email marketing.
- [ ] b. The acceptance of the privacy policy already allows the processing of personal data based on consent.
- [ ] c. For the consent to be valid, the data subject must actively mark the check-box.

8. The LGPD provides for the roles and responsibilities of the Processing Agents - the Controller and the Processor. With that in mind, carefully read the statements below and mark the alternative that **CORRECTLY** defines one of the Processing Agents:



- ☐ a. The Controller is the natural or legal person, public or private, who is responsible for decisions regarding the Processing of Personal Data.
- ☐ b. The Controller is the person who acts as a communication channel between the Data Subjects and the National Data Protection Authority ("ANPD").
- ☐ c. The Processor is a natural or legal person, governed by public or private law, who processes Personal Data on behalf of the Controller, which is the case, for example, of employees of a company, since they Process Personal Data on behalf of the company.

9. Carefully read the statements below, which refer to some of the definitions provided for in the LGPD, and select the **INCORRECT** alternative:



- ☐ a. Personal Data is any data that identifies or can identify an individual, for example: name, CPF, profession, registration, address, and bank information.
- ☐ b. Sensitive Data are confidential or secret Personal Data, such as CPF and salary.
- ☐ c. Processing of Personal Data means any and all activities carried out involving Personal Data and/or Sensitive Data, such as collection, access, storage, deletion, sharing and alteration.

10. Which of the following is a good data protection practice?

- [ ] a. Proper disposal of documents containing Personal Data that are no longer needed, by means of shredding or similar means.
- [ ] b. Installation of computer security software and use of appropriate computer security settings capable of protecting personal data from unauthorized access.
- [ ] c. All of the above.

BONUS QUESTION

Shall we test your knowledge of consent? Which of the scenarios below represent a valid consent?

- [ ] a. I have read and agreed to the Privacy Policy of Company Y, and therefore, I agree with any and all data processing to be performed by Company Y.
- [ ] b. I would like to receive personalized e-mails with offers and news from Company Y. You can unsubscribe at any time using the link found in each communication we send.
- [x] c. I would like to receive personalized e-mails with offers and news from Company Y. You can unsubscribe at any time using the link found in each communication we send.

ANSWERS

Question 1
Alternative C

The practice of direct marketing is controversial in Brazilian law, due to the omission of the LGPD on the subject and the absence of guidelines by the ANPD. However, it is understood that, depending on the relationship between the company and the client, it is possible to base the processing of data on legitimate interest (per article 7, IX, LGPD), and not only on consent (per article 7, I, LGPD). Note that, in order for legitimate interest to apply, a case-by-case analysis must be carried out, mainly to assess the expectations of the data subjects regarding the receipt of marketing actions, which may involve the need to prepare a Legitimate Interest Assessment ("LIA").

Question 2
Alternative B

The LGPD entitles the data subject to several rights, including confirmation of the existence of processing and access to the data (per article 18, I and II, LGPD). Therefore, depending on the request by the data subject, you must provide: (i) confirmation of the existence of processing or access to the data, in a simplified format and immediately; or (ii) a clear and complete statement, indicating the origin of the data, the lack of registration, the criteria used and the purpose of the processing, provided within 15 (fifteen) days from the date of the data subject's request (per article 19 LGPD). Note that, before responding to the data subject's request, you must observe if the rights in question do not violate commercial and industrial secrets, in which case the company must inform the data subject, in a justified manner, the reason for the refusal.

Question 3
Alternative A

Data processing activities (for example, collection) should be limited to the minimum necessary for the controller to be able to achieve the desired purpose, in this case, the registration on the platform and better identification of the data subject. If there is no specific purpose for collecting the data - regardless of whether it is a photo or other personal data - the processing activity will be deemed illegal under the terms of the LGPD. In fact, it is necessary for the company to inform the data subject, at the time of registration on the platform, about the purpose for the data's processing, in compliance with the duty of transparency.

Question 4
Alternative C

The LGPD stipulates that the data controller must inform the national authority and the data subject of the occurrence of a security incident that may entail significant risk or damage to data subjects (per article 48). Therefore, in view of the data breach that resulted in damage to data subjects due to the unauthorized disclosure of names and Taxpayer Numbers, the ANPD and the data subjects must be informed.

Question 5
Alternative A

The LGPD stipulates that the controller or the operator who, as a result of personal data processing activities, causes property, non-property, individual or collective damage to the data subject, in violation of personal data protection legislation, is required to repair such damage (per article 42 LGPD). In this regard, in order to guarantee indemnification of the data subject, the LGPD establishes that the controllers that are directly involved in the processing that resulted in damages to the data subject are jointly and severally liable, unless the controller proves that the damage caused cannot be attributed to him (per article 43 LGPD). It is worth mentioning that, in the event there are multiple controllers jointly and severally liable for the compensation of damages, the controller who bears the indemnity may recover such amount from the other controllers (per article 934 of the Civil Code).

Question 6
Alternative A

The LGPD establishes that the DPO must be appointed by the controller and his/her contact information must be publicly disclosed in a clear and objective manner, preferably on the controller's website (cf. article 41 LGPD). In addition, the LGPD does not determine the obligation of the DPO to have legal-regulatory knowledge, as provided for in the GDPR, which determines that the DPO should be appointed based on his professional skills and expertise on data protection laws (cf. MP No. 869/2018).

Question 7
Alternative C

Consent will be required whenever there is no other legal basis for Processing data. According to the LGPD, the consent of the data subject must be free, informed, and unequivocal (cf. article 5, XII, of the LGPD). Thus, the mere acceptance of the policy does not constitute active consent in relation to the Processing activity.

Question 8 Alternative A	According to article 5, VI of the LGPD, the Controller is the natural or legal person, public or private, who is responsible for decisions regarding the Processing of Personal Data. The Data Protection Officer ("DPO") is the one who acts as a communication channel between the data subjects and the ANPD (option "b"). Employees, in turn, cannot be considered Processors (option "c") as they do not process data in their own name, but on behalf of the company itself. It is important to note that, although employees are not considered Processor, they are also subject to the obligations of the LGPD, as they participate in the processing of personal data and must act in accordance with the principles and rules established by law.
Question 9 Alternative B	Sensitive Personal Data must not be confused with confidential or secret data. Sensitive Data is, in accordance with article 5, II of the LGPD, data on racial or ethnic origin, religious conviction, political opinion, membership of a union or organization of a religious, philosophical, or political nature, data referring to health or sexual life, data genetic or biometric, when related to a natural person.
Question 10 Alternative C	The measures contained in options (a) and (b) are considered good practices since they are in accordance with the principles of necessity and security established by the LGPD (Article 6, III and VII).
Bonus Question Alternative B	According to the LGPD, the data subject's consent must be free, informed and unequivocal (per article 5, XII, of the LGPD). Therefore, the consent obtained through the pre-selected checkbox (option "c") is not valid, as it does not ensure the holder full freedom of choice regarding the processing activity, since the data subject will not actively consent to the receipt of e-mails. In the same way, the consent to be provided by the data subject in the scenario presented in option "a" is not valid, because it does not refer to a specific purpose, but rather to a generic authorization for such processing (per article 8, § 4, of LGPD).



The Veirano Experience has a holistic, multidisciplinary, and business-oriented approach. In order to cover all the needs related to Compliance with LGPD, our Data Protection & Privacy team have developed several project formats, which comprise different scopes of work and meet specific demands of each client, whether national or international:

1. Full Compliance

With the performance of a multidisciplinary team, this project is aimed for clients whose goal is to identify and assess all ongoing processing activities within the company and based on that, identify vulnerabilities and structure an action plan for the creation of an effective privacy and data protection program based on legal, procedural, information security, and corporate governance pillars.

2. DPO as a Service

In this model, we take on the role of Data Protection Officer (DPO) on behalf of the client. To this end, we allocate a professional to perform the activities of managing and monitoring the client's data protection and privacy program.

3. M&A Legal Assistance

Designed to assist clients in the legal due diligence of merger and acquisition transactions, in order to identify relevant legal issues (red flags) and mitigate potential risks related to data protection and personal data security issues of the target company.

4. LGPD Pocket

A “pocket” advisory service for the adequacy of the activities and/or products developed by the company, regardless of its size or field of business, considering a reduced number of deliverables.

5. LGPD on Demand

LGPD On Demand is aimed at organizations that wish to have multidisciplinary advisory service on legal, information security, and corporate governance issues, with specific and timely action related to the protection of personal data.

6. LGPD Legal Helpdesk

The Helpdesk is designed to assist clients with LGPD legal consultations and demands within a monthly package of hours, either before, during, or after the initial compliance process.

7. Task Force For Security Incident Assessment And Reporting (VA Cybersecurity)

Specific and multidisciplinary legal advice in aspects related to the suspicion or occurrence of a security incident, in accordance with the most updated instructions from the ANPD and other applicable laws and regulations.

8. Representation in Administrative and Judicial Actions Involving Data Protection

Representation of clients in any administrative and/or judicial actions or potential actions involving data protection.

9. Analysis of Administrative and Judicial Decisions on Data Protection Matters

Periodic monitoring of decisions rendered in judicial and administrative proceedings involving the company or not, in order to present the authorities’ understanding and the impacts for the company or economic sector to the client in a summarized format.

10. Development and Updating of a Data Protection Impact Report

The ANPD may request from the controller to prepare a personal data protection impact report ("RIPD" or DPIA). Our team has expertise on the subject and can assist the company with the preparation and updating of the RIPD.

11. Development of Workshops

Development and application of training about the main concepts related to privacy and data protection to train its employees.

12. Playbook for Negotiating Commercial Contracts

Creation of playbooks for the negotiation of commercial contracts, to facilitate and speed up internal processes of commercial, technical, and legal teams.

13. Handbook to Reply the Data Subjetcs

Development of materials to assist the companies in prompt answering the data subjects' requests, as well as in the procedure to be followed by the company when answering the data subject, according to the business model developed by the company.

14. International Data Transfer

We help clients to understand the context of the international transfer, adapt it to the applicable legal basis, assess data localization requirements, add contracts, draft and review intra-group data sharing agreements, and generally respond to queries related to the harmonization of foreign with Brazilian regulations.

15. Privacy and Data Protection Auditing

We conduct audits to evaluate the company's level of maturity, presenting recommendations for risk mitigation.

16. Development and Review of Documents Pursuant to the Financial Sector

Our team has expertise in drafting security policies in accordance with the Central Bank's specific information security regulations, and in answering questions on the subject.

We are at your disposal in case of any questions or in the need of any additional information.



FÁBIO PEREIRA
+55 11 2313 5906
fabio.pereira@veirano.com.br



CINTIA ANDRADE
+55 21 3824 4655
cintia.andrade@veirano.com.br



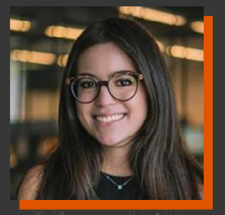
DENISE LOUZANO
+55 11 2313 5912
denise.louzano@veirano.com.br



ISABEL HERING
+55 11 2313 5726
isabel.hering@veirano.com.br



PAOLA LORENZETTI
+55 11 99976 8480
paola.lorenzetti@veirano.com.br



HELOISA HELENA DE PAULA CUNHA
+55 11 2313-3830
heloisa.cunha@veirano.com.br

This material was last updated on July 31, 2023 and published on August 04, 2023.
For more updated information please contact us.