Block 1 – PRINCIPLES OF THE LGPD

The General Data Protection Law Personal Data Protection (LGPD) is a regulatory framework that provides for the processing of data including in digital media, by an individual or by a person legal rights of public or private law, with the aim of protecting the rights of the fundamental rights of freedom and privacy and the free development of the personality of the natural person.

In this sense, the treatment of personal data must observe the principles, rights and guarantees provided for in the LGPD, regardless of the medium, physical or digital, or the technology used, such as Artificial Intelligence (AI) systems.

The development and use of AI systems should be guided by the observance of the principles that guide the personal data processing activities, among which the following stand out: Following:

(i) purpose, which limits the use of the data for legitimate, specific, explicit and informed purposes to the holder, without the possibility of further processing in a way that is incompatible with these purposes;

(ii) necessity, which requires that Only the data that is strictly necessary is used to achieve the purposes of the processing;

(iii) data quality, which guarantees the data subjects accuracy, clarity, relevance and updating of the data, according to the need and for the fulfillment of the purpose of its processing;

(iv) transparency, which requires the provision of clear, accurate and easily accessible information on the performance of the processing and the respective processing agents; and

(v) non-discrimination, which prohibits the Processing of personal data for unlawful discriminatory purposes or abusive.

(vi) accountability, and accountability, in which the agent must demonstrate the adoption of effective measures capable of proving the observance and compliance with the personal data protection standards and even the effectiveness of these measures.

These principles are essential for the development and responsible use of AI systems that respect the rights of the holders, avoiding excessive or inappropriate use of information Personal.

In this sense, The following question arises:

**1) How to make systems training compatible of AI with the principle of necessity, given that it is an activity that, Does it often require the processing of massive amounts of personal data? What safeguards can be adopted to ensure compliance with this principle and enable the appropriate development of AI systems; Considering, also, the importance of data quality and diversity Used?**

*The many new AI-driven uses for data, including sensitive personal information, raise privacy questions. They also offer the potential for more powerful and granular privacy controls for consumers. Accordingly, any policy framework should address the topics of privacy, consent, and modern technological capabilities as a part of the policy development process. Policy frameworks*

*must be scalable and assure that an individual's data is properly protected, while also allowing the flow of information and responsible evolution of AI. A balanced framework should avoid undue barriers to data processing and collection while imposing reasonable data minimization, consent, and consumer rights frameworks.*

*Further, Brazil's AI policy framework should utilize risk-based approaches to ensure that the use of AI aligns with any relevant recognized standards of safety, efficacy, and equity. Small software and device companies benefit from understanding the distribution of risk and liability in building, testing, and using AI tools. Policy frameworks addressing liability should ensure the appropriate distribution and mitigation of risk and liability. Specifically, those in the value chain with the ability to minimize risks based on their knowledge and ability to mitigate should have appropriate incentives to do so. Some recommended areas of focus include:*

- *Ensuring AI is safe, efficacious, and equitable.*
- *Encouraging AI developers to consistently utilize rigorous procedures and enabling them to document their methods and results.*
- *Encouraging those developing, offering, or testing AI systems intended for consumer use to provide truthful and easy-to-understand representations regarding intended use and risks that would be reasonably understood by those intended, as well as expected, to use the AI solution.*

**2) What good practices and safeguards must be observed in order to define purposes and the dissemination of clear, adequate information and easily accessible to data subjects regarding the processing of personal data carried out during the development and use of AI systems?**

*We recommend the following practices and safeguards be observed to define purposes and the dissemination of clear, adequate, and easily accessible information to data subjects regarding the processing of personal data carried out during the development and use of AI systems:*

- *Informing deployers and users of data requirements/definitions, intended use cases, populations, and applications (e.g., disclosing sufficient detail allowing providers to determine when an AI-enabled tool's use should reasonably be expected), and status of/compliance with all applicable legal and regulatory requirements.*
- *Prioritizing safety, efficaciousness, transparency, data privacy and security, and bias mitigation from the earliest stages of design, leveraging (and, where appropriate updating) existing AI/machine learning (ML) guidelines on research and ethics, leading standards, and other resources as appropriate.*
- *Where feasible, employing algorithms that produce repeatable results and that foster efficacy through continuous monitoring.*
- *Utilizing risk management approaches that scale to the potential likely harms posed in intended use scenarios to support safety, protect privacy and security, avoid harmful outcomes due to data biases, etc.*
- *Providing information that enables those further down the value chain to assess the quality, performance, and utility of AI/ML tools.*
- *Aligning uses with relevant ethical obligations and international conventions on human rights and supporting the development of new ethical guidelines to address emerging issues as needed.*

**3) How to make the principles of finality and transparency with the use of AI systems general purpose, that is, systems that can perform a wide variety of different tasks and serve different purposes?**

*Finality and transparency obligations for developers should be squarely tied to the intended and reasonably expected use cases, populations, and applications (e.g., disclosing sufficient detail allowing providers to determine when an AI-enabled tool's use should reasonably be expected). In other words, AI liabilities should only attach for demonstrated harms that a developer (1) has actual knowledge of or reasonable expectation on and (2) has the ability to take action to address.*

*Further, we strongly encourage finality and transparency obligations for developers and users to leverage risk management approaches that scale to the potential likely harms posed in intended use scenarios to support safety, protect privacy and security, avoid harmful outcomes due to data biases, etc.*

*Finally, the protection of intellectual property (IP) rights is critical to the evolution of AI. In developing approaches and frameworks for AI governance, policymakers should ensure that compliance measures and requirements do not undercut safeguards for IP or trade secrets.*

**4) What good practices and safeguards, as well as parameters or criteria, should be considered throughout of the entire lifecycle of AI systems to prevent unlawful discrimination or abusive?**

*The success of AI depends on ethical use. A policy framework must promote many of the existing and emerging ethical norms for broader adherence by AI technologists, innovators, computer scientists, and those who use such systems. Relevant ethical considerations include:*

- *Applying ethics to each phase of an AI system's life, from design to development to use.*
- *Maintaining consistency with international conventions on human rights.*
- *Prioritizing inclusivity such that AI solutions benefit consumers and are developed using data across socioeconomic, age, gender, geographic origin, and other groupings.*
- *Understanding that AI tools may reveal sensitive and private information about a user and ensuring that laws require the comprehensive protection of such information.*

Block 2 – LEGAL HYPOTHESES

The LGPD defines legal hypotheses, provided for in articles 7 and 11, which authorize the processing of personal data.

Several legal hypotheses can, in different contexts, support the processing of personal data throughout the AI system lifecycle. By way of example, one can mention the implementation of public policies, the protection of health, fraud prevention and the guarantee of the holder's safety and the execution of the contract.

Among the legal hypotheses that can be used in the context of AI, require further discussion or consent and legitimate interest.

Consent presupposes the obtaining a free, informed and unequivocal manifestation, through which the You agree to the processing of your personal data for a purpose determined, and may be

revoked later. Consent can be from difficult practical application in some contexts related to AI systems. Is the case, for example, of the collection of publicly accessible personal data through data scraping techniques aimed at training data scraping systems. WOULD.

In turn, legitimate interest may support the processing of personal data to meet legitimate interests of the controller or third parties, including the collectivity. To this end, the LGPD requires the adoption of a series of safeguards, including the definition of appropriate transparency measures and the performance of a balancing, as already addressed by the ANPD in the "Orientation Guide – Legitimate Interest".[1] A relevant limitation for the use of the legal hypothesis of legitimate interest in the context of the use of personal data for training AI systems stems from the fact that this legal hypothesis cannot be used to justify the processing of sensitive personal data.

In this sense, The following question arises:

**5) The processing of personal data in the context of AI systems can be supported by the legal hypothesis of the assent? Under what circumstances? What are the limitations for use of this legal hypothesis in these contexts and what safeguards should be Observed?**

*While the types of data items analyzed by AI and other technologies are not new, this analysis will provide greater potential utility of those data items to other individuals, entities, and machines. Thus, there are many new uses for, and ways to analyze, the collected data, offering the potential for more powerful and granular access controls for consumers. Accordingly, any policy framework should address the topics of privacy, consent, and modern technological capabilities as a part of the policy development process. Policy frameworks must be scalable and assure that an individual's data is properly protected, while also allowing the flow of information and responsible evolution of AI. This information is necessary to provide and promote high-quality AI applications. Finally, with proper protections in place, policy frameworks should also promote data access, including open access to appropriate machine-readable public data, development of a culture of securely sharing relevant data with external partners, and explicit communication of allowable use with periodic review of informed consent.*

*We appreciate that a suitable legal basis should exist for data processing under Brazilian law, whether AI is involved or not. We strongly caution Brazil against mirroring the approach taken by the European Union (EU) in hastily intervening into emerging and hyper-competitive AI markets, which has hampered innovation and damaged competition. Initially, we urge Brazil to focus on high-risk scenarios (e.g., health, safety) for which there is a clear evidence base to address (in other words, policy proposals should not be based on remote edge use cases or hypotheticals). The European Union's AI Act, like its Digital Markets Act (DMA), is unquestionably a protectionist anti-trade measure that Brazilian policymakers should carefully avoid aligning with. Further, the EU's AI Act is not fully implemented, nor is its impact on domestic and international digital commerce known. Brazilian policymakers should carefully track the implementation of AI regulation and its effects before mirroring the European Union's protectionist digital economy policies (which have not propelled the EU to global leadership in the digital economy to date). Brazil has the advantage of observing another major jurisdiction's experimental intervention into a nascent and dynamic digital economy and should fully capitalize on its opportunity to build on the lessons learned through the creation and implementation of AI regulation. On this basis alone, Brazilian government intervention into generative AI markets is ill-advised.*

*We strongly encourage Brazil to support pro-competitive dynamics in generative AI markets, which include lower overhead costs, greater consumer access, simplified market entry, and strengthened intellectual property protections for developers. Brazilian regulation of nascent markets, including with respect to digital platforms as well as potential new regulation of AI, creates barriers to Brazilian small business growth and job creation, ultimately creating significant trade barriers that harm Brazilian consumers.*

**6) Data processing in the context of AI systems, can be supported by the legal hypothesis of legitimate interest? Under what circumstances? If so, which ones safeguards must be adopted in these situations with a view to protecting rights of the data subjects, especially considering the prohibition of data processing sensitive persons based on the legal hypothesis of legitimate interest? In in particular, the collection of personal data for the training of AI systems, especially through data scraping techniques, can be based on the legal hypothesis of legitimate interest?**

*We appreciate that a suitable legal basis should exist for data processing under Brazilian law, whether AI is involved or not. We urge for the application of the LGPD in a technology neutral manner. Fundamentally, Brazilian policy should apply equally whether data is processed by AI or non-AI. As discussed above, layering on additional obligations or liabilities because of the use of AI will ultimately stifle innovation and distort competition, harm Brazilian small business growth and job creation, and harm consumers.*

*We strongly caution Brazil against mirroring the approach taken by the European Union (EU) in hastily intervening into emerging and hyper-competitive AI markets, which has hampered innovation and damaged competition. Initially, we urge Brazil to focus on high-risk scenarios (e.g., health, safety) for which there is a clear evidence base to address (in other words, policy proposals should not be based on remote edge use cases or hypotheticals). The European Union's AI Act, like its Digital Markets Act (DMA), is unquestionably a protectionist anti-trade measure that Brazilian policymakers should carefully avoid aligning with. Further, the EU's AI Act is not fully implemented, nor is its impact on domestic and international digital commerce known. Brazilian policymakers should carefully track the implementation of AI regulation and its effects before mirroring the European Union's protectionist digital economy policies (which have not propelled the EU to global leadership in the digital economy to date). Brazil has the advantage of observing another major jurisdiction's experimental intervention into a nascent and dynamic digital economy and should fully capitalize on its opportunity to build on the lessons learned through the creation and implementation of AI regulation. On this basis alone, Brazilian government intervention into generative AI markets is ill-advised.*

*We generally encourage Brazil to support pro-competitive dynamics in AI markets, which include lower overhead costs, greater consumer access, simplified market entry, and strengthened intellectual property protections for developers. Brazilian regulation of nascent markets, including with respect to digital platforms as well as potential new regulation of AI, creates barriers to Brazilian small business growth and job creation, ultimately creating significant trade barriers that harm Brazilian consumers.*

Block 3 – RIGHTS OF DATA SUBJECTS

The use of personal data in AI systems can have significant impacts on the rights of Holders.

One of the most critical aspects says decision-making based solely on the automated processing of personal data and that may produce legal effects or impact significantly the interests of individuals. The LGPD establishes that the data subject of the data has the right to understand the criteria used for this decision and, more specifically, to request a review when such decisions affect interests. This seeks to avoid or mitigate possible errors, biases or unlawful or abusive discrimination that may arise from automated decisions that negatively affect the individual.

The use of personal data in AI systems also require careful consideration of the possible negative impacts on the data subject, which may occur in decisions aimed at define your personal, professional, consumer and credit profile or the aspects of his personality.

Still in relation to the exercise of the rights, the confirmation of the existence of processing, access to personal data, the correction of incomplete, inaccurate or outdated data, the anonymization, blocking, or deletion of unnecessary, excessive, or Treaties in non-compliance with the provisions law,inaddition to the possibility of repealing the assent. The holder may also oppose to the treatment carried out on the basis of one of the hypotheses of waiver of consent, in case of non-compliance with the provisions of the LGPD.

LGPD compliance does not not only establishes a protection framework for data subjects, but also strengthens their confidence in the development and use of AI systems; ensuring that technological advancement is always aligned with the protection of fundamental rights and privacy.

In this sense, The following question arises:

**7) How do the rights of the holder, provided for in the LGPD, apply to AI systems?**

*We urge for the application of the LGPD in a technology neutral manner. Fundamentally, Brazilian policy should apply equally whether data is processed by AI or non-AI. As discussed above, layering on additional obligations or liabilities because of the use of AI will ultimately stifle innovation and distort competition, harm Brazilian small business growth and job creation, and harm consumers.*

**8) What are the good practices and the safeguards to be observed in the provision of customer service channels holder to exercise their rights, such as rights of access, opposition and review of automated decisions, in the context of data processing by AI systems? If possible, describe the tools used for the implementation of such service channels, with the respective parameters Used.**

*Brazil's policy framework should prioritize providing the flexibility for AI developers to innovate in response to consumer demands, while applying the LGPD in a technology neutral manner. We agree that frameworks for AI should address the topics of privacy, consent, and modern technological capabilities as a part of the policy development process. Such policy frameworks must be scalable and assure that an individual's data is properly protected, while also allowing the*

*flow of information and responsible evolution of AI. A balanced framework should avoid undue barriers to data processing and collection while imposing reasonable data minimization, consent, and consumer rights frameworks; evolving standards should be monitored and deferred to (e.g., self-attestation to such standards could provide a safe harbor to enforcement).*

**9) There must be safeguards and specific limits for the processing of sensitive personal data and for the processing of personal data of children, adolescents and the elderly during the stages of the life cycle of AI systems?**

*With respect to safeguards and specific limits for the processing of sensitive personal data and for the processing of personal data of children, adolescents, and the elderly during the stages of the life cycle of AI systems, frameworks must be scalable and assure that an individual's data is properly protected, while also allowing the flow of information and responsible evolution of AI. A balanced framework should avoid undue barriers to data processing and collection while imposing reasonable data minimization, consent, and consumer rights frameworks; evolving standards should be monitored and deferred to (e.g., self-attestation to such standards could provide a safe harbor to enforcement).*

*We urge for the application of the LGPD in a technology neutral manner. Fundamentally, Brazilian policy should apply equally whether data is processed by AI or non-AI. As discussed above, layering on additional obligations or liabilities because of the use of AI will ultimately stifle innovation and distort competition, harm Brazilian small business growth and job creation, and harm consumers.*

**10) What are the requirements to be for the guarantee and application of the right to review decisions (art. 20 of the LGPD)? What can be considered as a decision made solely on the basis of automated processing of personal data? What interests could be affected?**

*Absent a demonstrated need for alternative policy changes to address the application of LGPD Article 20 in the context of AI, the application of the LGPD should be done in a technology neutral manner. Fundamentally, Brazilian policy should apply equally whether data is processed by AI or non-AI. As discussed above, layering on additional obligations or liabilities because of the use of AI will ultimately stifle innovation and distort competition, harm Brazilian small business growth and job creation, and harm consumers.*

**11) In what hypotheses and under which conditions may require human review of automated decisions with a view to adequately guaranteeing the rights of data subjects?**

*Brazil's approach should utilize risk management approaches that scale to the potential likely harms posed in intended use scenarios to support safety, protect privacy. and security, avoid harmful outcomes due to bias, etc. In higher risk use cases, human review of automated decisions may be appropriate, but this will not always be the case and the application of the LGPD should not mandate universal requirements for such reviews. We also urge for alignment with recognized standards of safety, efficacy, and bias mitigation where possible.*

*Small software and device companies benefit from understanding the distribution of risk and liability in building, testing, and using AI tools. Policy frameworks addressing liability should ensure the appropriate distribution and mitigation of risk and liability. Specifically, those in the value chain*

*with the ability to minimize risks based on their knowledge and ability to mitigate should have appropriate incentives to do so.*

**12) What parameters to be observed for the provision of clear and adequate information regarding the criteria and procedures used for automated decision-making, in the terms of paragraph 1 of article 20 of the LGPD? What Limits and Secret Parameters justify the non-observance of the supply of information, as provided for in the same legal provision?**

*Finality and transparency obligations for developers should be squarely tied to the intended and reasonably expected use cases, populations, and applications (e.g., disclosing sufficient detail allowing providers to determine when an AI-enabled tool's use should reasonably be expected). In other words, AI liabilities should only attach for demonstrated harms that a developer (1) has actual knowledge of or reasonable expectation on and (2) has the ability to take action to address.*

*Further, we strongly encourage finality and transparency obligations for developers and users to leverage risk management approaches that scale to the potential likely harms posed in intended use scenarios to support safety, protect privacy and security, avoid harmful outcomes due to data biases, etc.*

*Finally, the protection of intellectual property (IP) rights is critical to the evolution of AI. In developing approaches and frameworks for AI governance, policymakers should ensure that compliance measures and requirements do not undercut safeguards for IP or trade secrets.*

**Block 4 - GOOD PRACTICES AND GOVERNANCE**

Governance and the adoption of good practices in the use of personal data in AI systems can be a good strategy by processing agents to ensure the protection of rights of data subjects and compliance with the LGPD.

The adoption of security measures appropriate and compatible with the risk involved in each situation, in order to Prevent the occurrence of security incidents and mitigate potential impacts negative effects on data subjects are mechanisms provided for in the LGPD system that should be adopted throughout the lifecycle of AI systems that use personal data. In this sense, article 46, paragraph 2, of the LGPD, determines that Safety measures must be observed from the design stage of the product or service until its execution, a rule that is also applicable to the context of the development and use of AI systems.

Similarly, article 50 of the LGPD provides that processing agents may formulate rules of good practices and governance that establish the conditions of organization, the procedures, including complaints and petitions from holders, safety standards, technical standards, obligations specific to the various people involved in the treatment, the educational actions, the internal mechanisms for supervision and risk mitigation and other aspects related to the processing of personal data. In addition, paragraph 2, I of the same Article establishes the minimum requirements for the implementation of the privacy governance.

In this regard, it is important to highlight that the use of safeguards, such as anonymization techniques, can provide greater protection for data subjects, who allow the processing of

information without these can be associated with a specific individual. Anonymization is a technique that helps minimize risk and protect privacy, especially in the training of AI models, in which large volumes of data are used, may contain information that allows for potential risks to civil liberties and to the fundamental rights of the holders.

Other relevant mechanism provided for in the LGPD and which can be used for the governance and management of risks in the context of the development and use of AI systems is the report of impact on the protection of personal data (RIPD). If well prepared, a DPIP can provide the organization with appropriate tools for risk awareness involved and the mitigation measures adopted in the case, in addition to allowing the accountability regarding the system.

In this sense, AI governance it involves, among other actions, the implementation of policies and processes that ensure comprehensive compliance with standards and good practices relating to the protection of personal data and guide how personal data should be be collected, processed, stored, and used throughout the entire cycle of life of an AI system.

Thus, the following questions are asked:

**13) How do programs privacy governance can be used as a mechanism to promote the compliance of the development and use of AI systems with the LGPD? What requirements, specifically related to the development and use of systems of AI, should be observed in these cases?**

*Absent a demonstrated need for alternative policy changes to address the application of LGPD compliance in the context of AI, the application of the LGPD should be done in a technology neutral manner. Fundamentally, Brazilian policy should apply equally whether data is processed by AI or non-AI. As discussed above, layering on additional obligations or liabilities because of the use of AI will ultimately stifle innovation and distort competition, harm Brazilian small business growth and job creation, and harm consumers.*

*This said, Brazil should encourage design of AI systems that are informed by real-world workflows, human-centered design and usability principles, and end-user needs. A framework enabling the scaling of risk mitigation to the reasonably expected and intended harms presented by intended use cases will enable such design practices as appropriate. AI systems should facilitate a transition to changes in the delivery of goods and services that benefit consumers and businesses. The design, development, and success of AI should leverage collaboration and dialogue among users, AI technology developers, and other stakeholders to have all perspectives reflected in AI solutions.*

**14) Considering the principle of accountability and accountability, what information must be documented during the cycle of life of an AI system? In what specific contexts related to AI systems: is it recommended to prepare DPRIs? In this case, it is possible establish specific requirements to be observed in the preparation of the RIPD?**

*Absent a demonstrated need for alternative policy changes for LGPD documentation and compliance in the context of AI, the application of the LGPD should be done in a technology neutral manner. Fundamentally, Brazilian policy should apply equally whether data is processed by AI or non-AI. As discussed above, layering on additional obligations or liabilities because of the use of AI will ultimately stifle innovation and distort competition, harm Brazilian small business growth and*

*job creation, and harm consumers. Therefore, at this time we discourage new mandates for AI-specific documentation requirements absent a well-demonstrated need for them; however, we do support guidance on LFPD compliance related to AI uses that affirms a technology neutral application of the law.*

15) Considering the life cycle of an AI system, at what time and context of the processing would be feasible or Anonymization necessary? What technique is used? What other measures of security could eventually be used to protect privacy of data subjects?

*Depending on the use case(s) and intended/expected uses, the timing and context of processing, and the feasibility of anonymization, will vary. A wide variety of technical protection mechanisms are used today to protect the privacy of data subjects, while further tools and approaches are constantly being developed. We encourage Brazil to avoid technology-specific mandates by relying on outcome-based measures of compliance, which will permit AI developers and deployers to tailor their risk management approaches to intended/expected subjects and use cases.*