Annex I

Main Topics	GDPR	LGPD	Our Comments
Legal Basis for Processing of Sensitive Data	Personal data is any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a 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.	Personal data is any information relating to an identified or identifiable natural person.	The LGPD does not bring examples of personal data in its definition. In this case, we may assume that the Brazilian Data Protection Authority (In Portuguese, "Autoridade Nacional de Proteção de Dados" or "ANPD") might regulate this matter and determine the concept of "identifiable natural person". If not, a case-by-case analysis will be necessary.
Principles	The principles are: • Lawfulness, fairness and transparency; • Purpose limitation; • Data minimization; • Accuracy; • Storage limitation; • Integrity and confidentiality; • Accountability.	The principles are: • Purpose; • Adequacy; • Necessity; • Free access; • Data quality; • Transparency; • Security; • Prevention; • Liability and accountability; • Non-discrimination.	The LGPD establishes the non-discrimination principle, which precludes the processing for illegal, abusive or discriminatory purpose.
Legal Basis for Processing of Personal Data	There are six lawful basis: • Consent; • Legal obligation; • Life protection and vital interests; • Public interest; • Performance of a contract; • Legitimate interests.	There are ten lawful basis: • Consent; • Legal or regulatory obligation; • Performance of a contract; • Implementation of public policies by the Public Administration; • Studies by research entities; • Establishment, exercise or defense of legal claims; • Life protection and vital interests; • Health protection; • Legitimate interests; • Protection of credit.	The LGPD provides a **wider scope** for the lawful basis for processing personal data. However, most of the additional legal bases would fall under the GDPR's legitimate processing of data.

Main Topics	GDPR	LGPD	Our Comments
Legal Basis for Processing of Sensitive Data	There are ten lawful basis: • Explicit consent; • Collective agreement; • Legal obligation; • Life protection; • Substantial public interest; • Legitimate interests (a foundation, association or other not-for-profit body with a political, philosophical, religious or trade union aim, processing data about its members); • Manifestly made public by the individual; • Establishment, exercise or defense of legal claims; • Archiving, scientific or historical research purposes; • Preventive or occupational medicine, assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment.	There are eight lawful basis: • Explicit and distinct consent; • Legal or regulatory obligation; • Necessary by the Public Administration for the execution of public policies; • Research purposes; • Regular exercise of rights, including in a contract and in a judicial, administrative and arbitration procedure; • Life protection; • Protection of health, in a procedure carried out by health professionals or by health entities; • Prevention of fraud and the safety of data subject, in processes of identification and authentication of registration in electronic systems.	The LGPD provides a **wider scope** for the lawful processing of sensitive personal data. The LGPD establishes two important legal basis for the processing of sensitive data: • **Regulatory obligation** (Governmental Agencies can provide regulations for the processing of sensitive data, for example: processing health data); • **Regular exercise of rights, including in a contract** (an employer can collect biometric information from its employees based on the employment contract, as long as it relates to the labor relationship).
Health Sensitive Data	The GDPR does not establish any prohibition regarding the communication or shared use of sensitive health data.	The communication or shared use of sensitive health data between controllers with the purposes of obtaining economic advantages is prohibited, except for: • Data portability requested by the data subject; or • Adequate provision of supplementary health services.	The LGDP establishes **stricter requirements** for the communication or shared use of sensitive health data.

Main Topics	GDPR	LGPD	Our Comments
Legitimate Interests	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 (Recital 47).** Such legitimate interest could exist for example where there is a **relevant and appropriate relationship** between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller.	The legitimate interests of a controller or a third party are a legal basis for processing, if the rights and freedoms of the data subject are not overriding, taking into consideration the support and promotion of the controller's activities.	The LGPD is **more flexible** than the GDPR on this matter, since legitimate interests can be used as a legal basis for processing data for the "support and promotion of the controller's activities".
Anonymized data	Outside of the scope of the law (reasonable steps to re-identify).	Outside of the scope of the law (reasonable steps to re-identify).	The regulation on this matter is **very similar** in both the LGPD and the GDPR.
Pseudonymized data	Within the scope of the law (information on an identifiable natural person).	Not defined by the law, except for **research undergone by public health agencies.**	The LGPD only provides a definition for pseudonymized data in the **specific context of research in public health.**
Right to have automated decisions reviewed	The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.	The data subjects have the right to request the revision of automated decisions.	The regulation on this matter is **very similar** in both the LGPD and the GDPR.

Main Topics	GDPR	LGPD	Our Comments
Scope of the Law	Any company that has a branch in the EU or offers services to the EU market and collects and processes personal data of data subjects located in the EU, regardless of the nationality, will be subject to the new law.	Any company offers services to the Brazilian market and collects and processes personal data of subjects located in the country, regardless of the nationality, or if data is processed within the Brazilian territory, will be subject to the new law. Data flows that are considered in transit to other countries or merely transmitted into Brazil, but not further shared with processors in Brazil, do not fall within the scope of the law.	Both regulations offer a **high level of protection** to individuals in Brazil or in the EU. In some cases, due to the extraterritorial effects of the LGPD and the GDPR, organizations may be subject to both regulations simultaneously.
Data Access Requests	Up to 30 days. Gratuity is optional.	Up to 15 days. Gratuity is mandatory.	The LGDP establishes **stricter requirements** for companies to comply with data access requests.
Representative of Controllers not established in the region	The Controller or the Processor shall designate a representative.	There is no legal obligation to designate a representative in Brazil.	The LGDP establishes **more flexible requirements.** There is no legal obligation to designate a representative of the Controller within the national territory.
Registration of Processing Activity	Not mandatory for companies with less than 250 employees.	Mandatory for all companies.	The LGDP establishes **stricter requirements.**
Data Breach Notification	Within 72 hours.	Within a **reasonable time,** describing all the data affected by the breach, the risks related, and the technical and security measures related to the incident.	The LGPD does not set forth a specific deadline for notification in cases of data breach.
Data Protection Authority or ANPD	Should be defined and established at the national level.	The Brazilian President enacted the Provisional Measure No. 869 (December 28, 2018) and created the ANPD.	According to the Provisional Measure, the ANPD should be an administrative body, with technical autonomy, but no financial but budgetary autonomy, connected to the Cabinet of the Presidency. The absence of financial and budgetary autonomy could jeopardize the authority's autonomy.

Main Topics	GDPR	LGPD	Our Comments
Data Protection Officer (DPO)	It is not mandatory to all controllers. Conditions can be volume and type of data processed, use of new technologies and risks to data subjects.	It is mandatory to all controllers, regardless of the size, type and volume of the data processed and risks to data subject (to be further regulated by the ANPD).	The GDPR has regulated the matter with more details than the LGPD. In this sense, we expect further regulations on the role and tasks of a DPO in Brazil.
International Data Transfer	The transfer of personal data to third countries or international organizations may take place when an **adequate level of protection** is ensured. In the absence of an adequacy decision, a transfer can take place through the provision of appropriate safeguards and on condition that enforceable rights and effective legal remedies are available for individuals.	The transfer of personal data to third countries or international organizations will only be permitted: • To countries with an **adequate level of protection;** • Through the use of standard contractual clauses, global corporate rules, seals, certificates and codes of conduct approved by national data protection authority; • With the **consent** of the data subject.	The regulation on this matter is very similar in both the LGPD and the GDPR. Notwithstanding, unlike the GDPR, the **LGPD does not establish any derogations from the international data transfer requirements.** In the LGPD, legitimate interests are not a legal basis for international transfers.
Fines	Up to 4 percent of global revenue of the economic group (up to € 20 million).	Up to 2 percent of the Brazilian revenue of the economic group (up to BRL 50 million).	The fines under LGPD have **lower limits** compared to GDPR.