# Data protection in Brazil: The first analysis of the matter by the Consumer Protection Department

**Authors:** **Leonardo A. F. Palhares** lpalhares@almeidalaw.com.br **Caio Iadocico de Faria Lima** cilima@almeidalaw.com.br

The importance of data protection and privacy is indubitable, particularly considering the current economic model of the internet that provides free access to applications in exchange for users' data, which is extremely valuable to any company that seeks to negotiate them for several purposes (from advertising to the creation of databanks for the analysis of credit and risk assessment of operations).

However, even before the bill reached the National Congress, the Consumer Protection Department ("Departamento de Proteção e Defesa do Consumidor" – DPDC), major organization of consumer protection at federal level in Brazil, issued a decision concerning the matter, which deals with irregularities on storage politics and processing access registry and personal data from consumers in internet applications[1].

On this decision, the DPDC presented its view in an unprecedented manner regarding several topics currently discussed by the market, assuming a position that will be extremely important to the development of the matter in Brazil.

The DPDC approached main questions involving data protection that are recurring in global discussions, such as collection, storage, register, vigilance, processing and disclosure of users' personal data. To address these questions, the department used concepts, principles and common rules to consumer protection in order to justify their understanding in relation to personal data protection, as noted next.

● ***Data treatment and its relevance***

The management of personal data involves different steps during the business operation of any company, as mentioned above. The DPDC tried to provide directives and specific rules to each of the steps.

With regards to such moments, it is known that data collection occurs while obtaining personal data from the holder, either voluntarily (through the filling of a form) or indirectly (as in cases of companies that receive information from third parties for analysis and classification of risks in an operation).

Vigilance is not related to the personal data itself; it is related to how users use a service. Whenever such information is targeted for tracking and registering, they gain value, especially when allied to consumption patterns and to the personal data obtained with the collection.

Lastly, it is necessary to explain the concept regarding treatment and disclosure of information. Data processing includes operations that allow any kind of use of personal data (including collection, storage, planning, conservation and modification) as well as its disclosure to third parties.

Each of the moments of the personal data value chain has vital importance in the relation between holder and data manager. Currently, several companies obtain access to data directly from their users, but do not explain how they intend to store it and process it during the relation. In this sense, some users end up not having any knowledge that their personal data can and, as a matter of fact, is shared with third parties that will exploit it commercially.

In consideration of these facts, we analyzed the DPDC's decision below.

● ***DPDC's understanding***

[1] Oi, a telecommunications company, was punished in Administrative Processing No. 08012.003471/2010-22, with penalty of R$3.500.000,00 (three million and five hundred thousand Brazilian Reais, approximately $1.6 million U.S. dollars) for alleged violations to consumer protection rules that were related to personal data protection.

On the Technical Note issued by the DPDC, the government body tried to approach most of the subjects related to data protection.

*Collection:* regarding the rules of personal data collection, the DPDC affirmed that the collection must be ruled by the customers' guarantee of access to information, meaning that, all information should be made available in the moment of the register, record and/or personal and consumption data, foreseen in the Consumer Protection Code[2], (which deals specifically with negative registration of consumers, but is interpreted analogously in this case to justify the creation of a database in general). Thereby, with the expansion of the understanding of these rules set forth by the DPDC, users will have to be properly informed whenever a company creates a registry of their data or activity.

*Treatment and disclosure:* Regarding the treatment, limitations were established for the moment of presentation and acceptance of the services related to personal user data. According to the DPDC, the holder of the information must be properly informed of data treatment operations pursuant to constitutional and basic consumer protection principles, namely: (i) the right to access to information[3]; (ii) objective good faith[4] and transparency[5] and (iii) the vulnerability of consumers[6].

Thus, a company that provides any kind of service or application, must inform the consumer in a proper and transparent manner, clearly and unequivocally how they intend to use the obtained information, including if their intention is to disclose it to third parties. In this sense, the disclosure of information is not directly prohibited by the DPDC, but companies have the obligation to inform the data holder if it occurs, and the holder must consent with such disclosure.

*Vigilance:* besides that, the analysis of the registration of activities was studied by the department of consumer protection, which classified the non-informed vigilance "of constant manner of consumer browsing online" as a clear violation to the principle of objective good faith between the parties. Still regarding vigilance, the DPDC also presented arguments that reinforce the principles of data protection, in accordance to the Brazilian Internet Framework ("Marco Civil")[7]: the right to the inviolability of intimacy, privacy and secrecy of communications online.

***

The DPDC tried to address the questions and urges it thought to be most important at the moment, and further highlighted rules and basic principles that must be followed by companies that perform any kind of management and/or personal data treatment.

Some providers may need adjustments in their politics in order to abide to these basic principles. They will have to present information to consumers regarding an eventual possibility of any unusual activity concerning the users' data.

Therefore, the violation of the principles described above, in each one of the steps of personal data management is subject to penalties that will vary according to (i) the severity of the infringement, (ii) the economical advantage obtained, and (iii) the economic condition of the agent, according to the Consumer Protection Code[8].

Based on the arguments above, the DPDC took the first step to set general guidelines related to personal data protection and to alert all companies that currently perform this type of collection and data treatment in Brazil.

Almeida Law has a team specialized in Personal Data Protection and Privacy that closely follows the legislative process in the country concerning the questions depicted herein, and has been leading debates regarding these new rules, in

[2] Art. 43, Consumer Protection Code.
[3] Art. 5, XIV, Federal Constitution.
[4] Art. 4, III, Consumer Protection Code.
[5] Arts. 6, II, III and IV, e 31, Consumer Protection Code.
[6] Art. 4, I, III, Consumer Protection Code.
[7] Art. 7º, Brazilian Internet Civil Rights Act (L. 12.965/14).
[8] Art. 57, Consumer Protection Code.

addition to providing legal advice to clients that perform management and direct or indirect treatment of personal data.