20th Edition | 2022

# cybernews.

Tozzini Freire.
ADVOGADOS

# *index*

///// Brazilian Context

# The Brazilian Data Protection Authority takes another step in regulating the application of sanctions

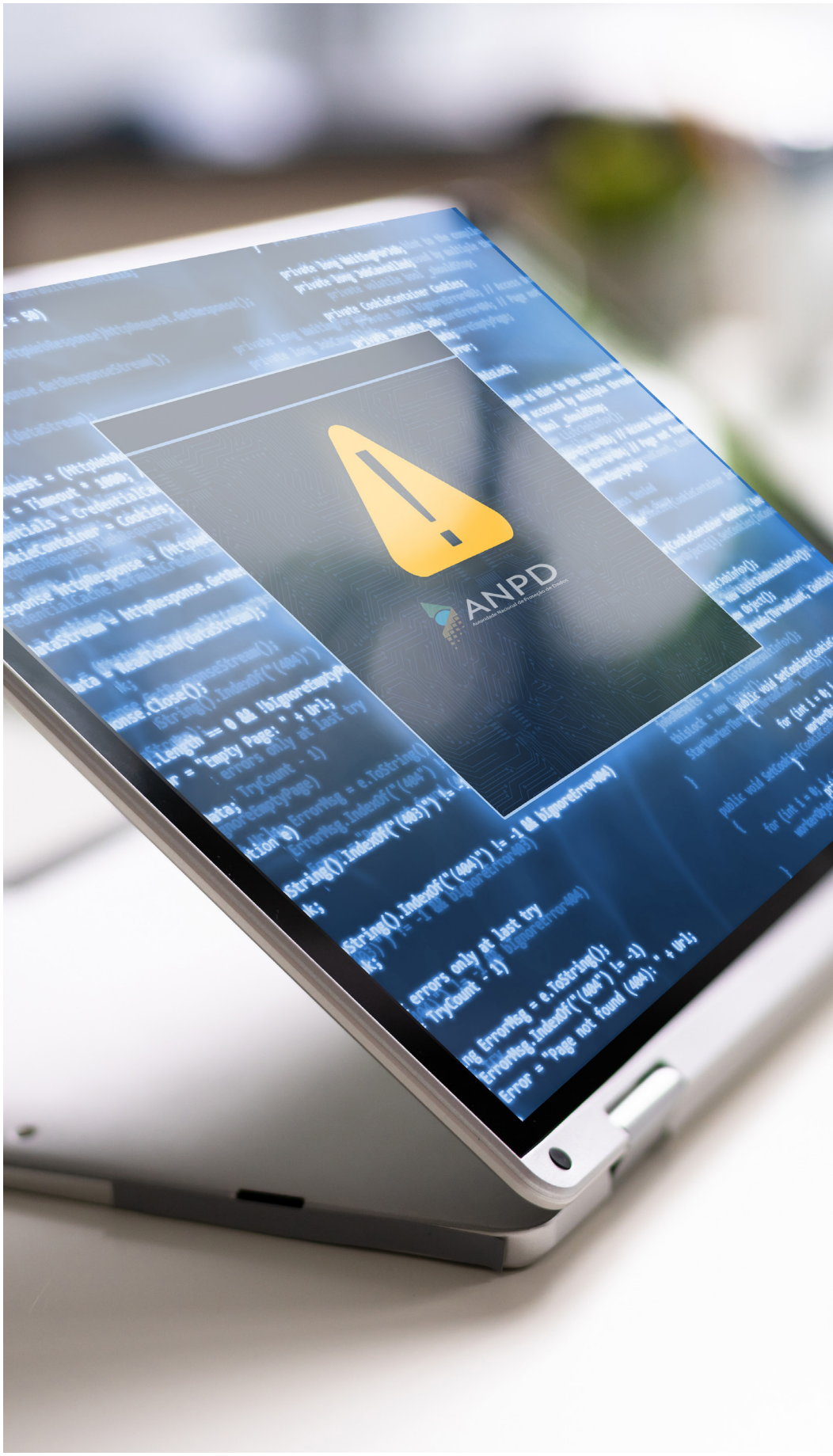
The Brazilian Data Protection Authority (ANPD) has launched a public consultation on the draft Resolution that regulates the application of sanctions outlined in Articles 52 and 53 of the Brazilian General Data Protection Law (LGPD).

The proposed rule aims to complement the Regulation of the Inspection Process and the Sanctioning Administrative Process, approved by Resolution CD/ANPD No. 1/2021, by establishing clear rules, in particular the parameters and criteria, for the application of administrative sanctions, i.e., the sanctions dosimetry.

Contributions must be sent through the Participa Mais Brasil platform and can be submitted until September 15, 2022.

We highlight that the ANPD has also published the Regulatory Impact Analysis Report, which details the parameters and criteria for the application of sanctions and calculation of fines, as well as the votes casted by the Authority's directors.

These initiatives are in line with the ANPD's regulatory agenda, which provided for the start of the regulation of the supervision and sanctioning rules still in 2022



## Recommendation 34/2022 on best practices to be adopted to mitigate risks related to cybersecurity

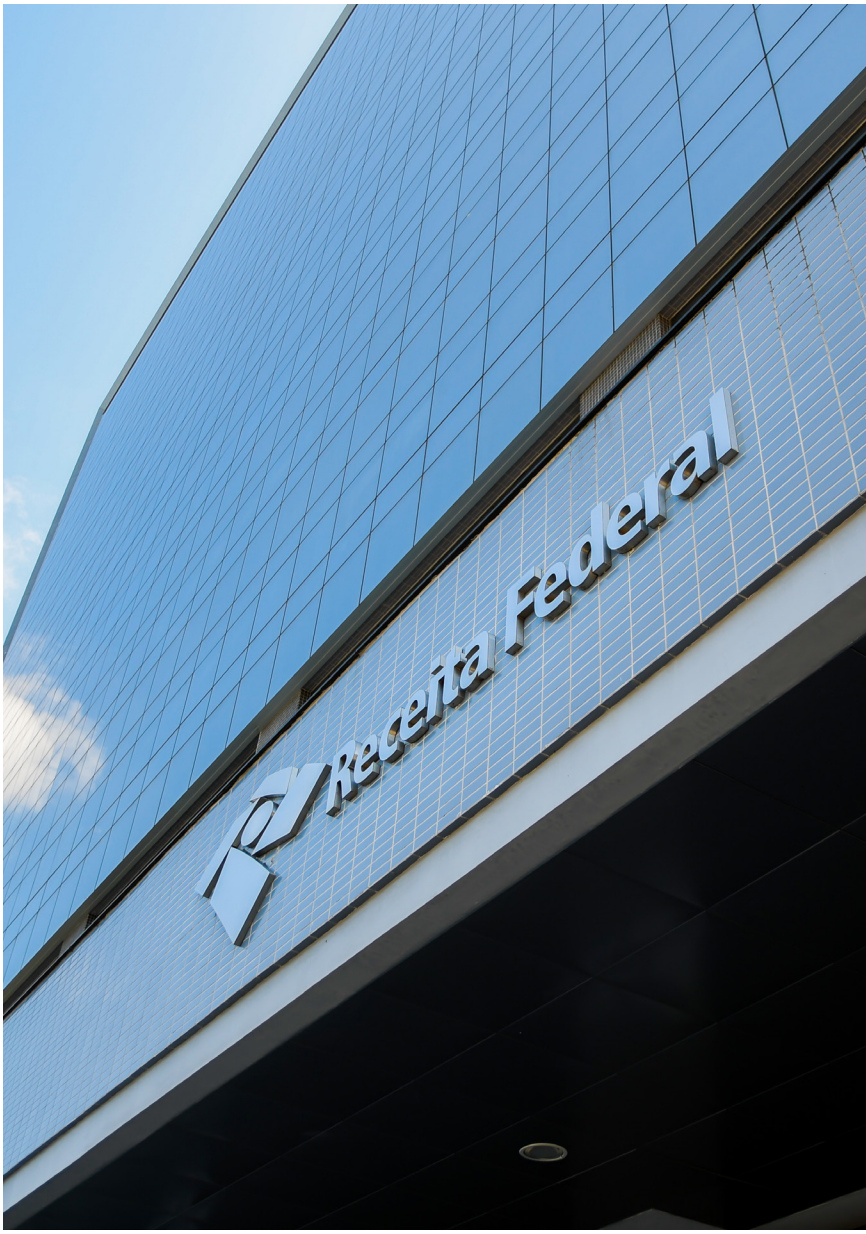
On September 8, 2022, the Government Center for Prevention, Processing, and Response to Cyber Incidents (CTIR Gov) among with the Digital Government Office (SGD) and the Brazilian Data Processing Service (SERPRO) issued Recommendation 34/2022 on best practices to mitigate the main cybersecurity risks.

The COVID-19 pandemic has intensified remote working and, consequently, the cybersecurity concern as well, which justifies the relevance of being aware of these preventive measures.

Regarding policies, it was recommended to establish plans for backup management with secure data storage, updating computer systems, remote access security when the organization uses VPN and double/multiple factor authentication, and corporate devices monitoring policy.

Besides these measures, performing periodic data backup tests, periodically reviewing strategic security plans and cyber and information security policies, using strong passwords, and keeping a centralized record of system events (logs) in a controlled environment were also actions recommended by the authorities.

## ANPD publishes a Technical Note that concludes the analysis of the data processing between the Federal Revenue and SERPRO




On August 5, 2022, the ANPD published Technical Note No. 68/2022/CGF/ANPD, which deals with the analysis carried out by the ANPD after the publication of Ordinance RFB No. 167/2022, of April this year, which authorizes the Federal Data Processing Service (SERPRO) to provide access to data and information from the Internal Revenue Service for third parties.

In short, the note discloses the end of the inspection procedure, concluding that there is no incompatibility in the data processing operated by Ordinance RFB No. 167/2022 with the provisions of the personal data protection legislation. In this sense, the ANPD concluded, through the Impact Reports presented by the Federal Revenue, that the aforementioned Ordinance aims to provide the necessary instruments for access to data that were already, for the most part, public data by virtue of regulations and public policies, such as information like CPF (Brazilian Individual Taxpayer Registry), CNPJ (Brazilian Register of Legal Entities) and debt clearance certificate.

Therefore, there was no incompatibility with the LGPD of the data processing presented by Ordinance RFB No. 167/2022, given that these are personal data that are included in public policies and have a defined purpose.

## ANPD starts the process to obtain subsidies for the processing of high-risk personal data

The ANPD started, on August 29, 2022, the new process to obtain subsidies for the processing of high-risk personal data, which will be open for contributions that must be sent through the Participa Mais Brasil platform until September 29, 2022 (click here).

This process to obtain subsidies is based on Article 4 of the Regulation on the application of the LGPD for small processing agents, approved by CD/ANPD Resolution No. 2, dated January 27, 2022, which establishes the criteria for defining high-risk processing to the data subject.

Article 4 provides that personal data processing will be considered high-risk when it complies cumulatively with at least one general and one specific criterion. Among these, the general criteria are processing of personal data (a) on a large scale, or (b) that could significantly affect the interests and fundamental rights of the data subjects.

Specific criteria may be processing with (a) the use of emerging or innovative technologies, (b) surveillance or control of publicly accessible areas, (c) decisions taken solely based on automated processing of personal data, or (d) use of sensitive personal data or personal data of vulnerable groups, such as children, teenagers, and seniors.

## ANPD starts the process to obtain subsidies for the processing of children's and adolescents' data

The ANPD opened, on September 8, 2022, the new grant taking on the processing of personal data of children and adolescents, which will be open for contributions that must be sent through the Participa Mais Brasil platform until October 7, 2022 (click here).

As published by the ANPD, this subsidy collection aims to analyze which legal hypothesis would apply to children's and adolescents' personal data processing. Although the LGPD provides a specific section for the processing of data on children and adolescents, there are still controversies about the correct interpretation of certain provisions of the law by professionals in the area.

In this sense, due to the legal uncertainty arising from the lack of definition of which legal hypothesis authorizes the processing of children and adolescents' personal data, the ANPD structured a preliminary study on the subject, to foster public debate and support future decision-making on the matter by the ANPD.

In this way, given the divergences found and the importance of the topic, the ANPD started the process to receive contributions from society, in order of collecting opinions from people interested in the subject, so that multiple perspectives are taken into account in the regulation of the matter.

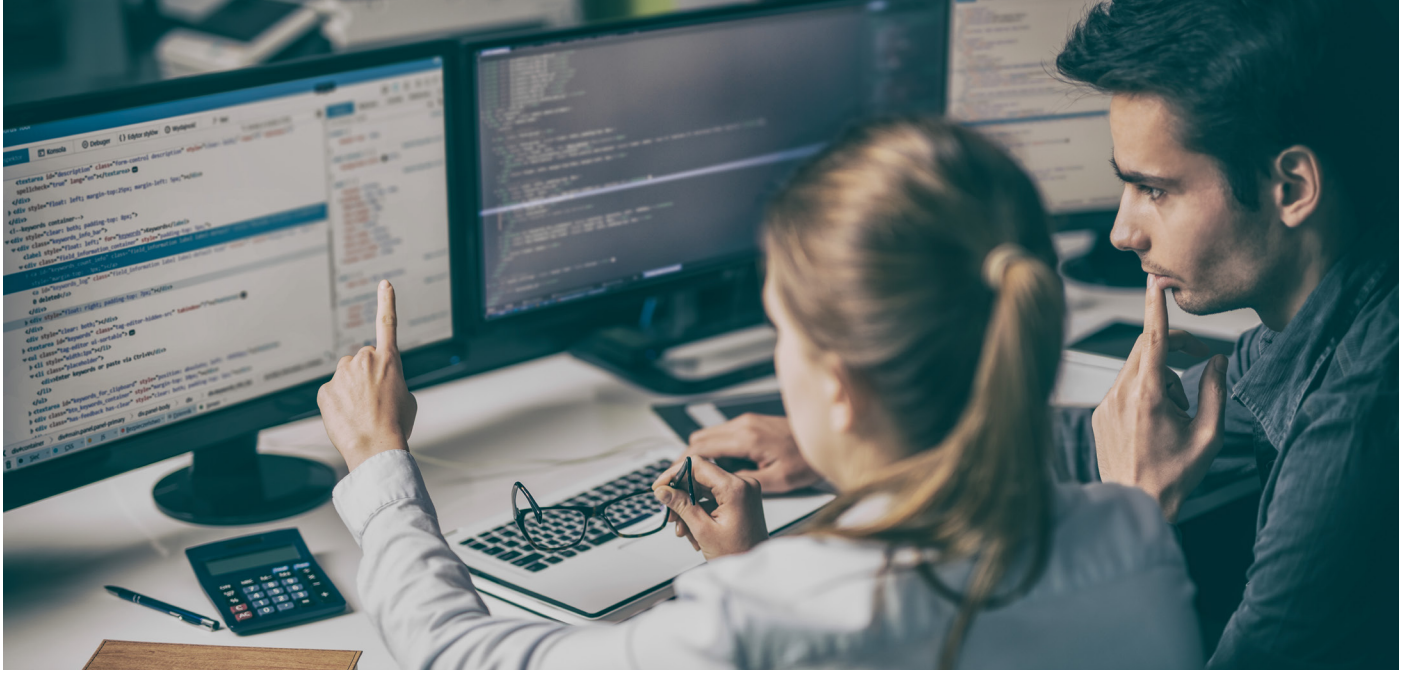
# Guideline 3/2022 on “Dark patterns” in social media platform interfaces: How to recognize and avoid them

Firstly, the term “dark patterns” was created in 2010 by the British scientist Harry Brignull, to refer to the design strategies used to promote behavior contrary to the laws of protection of personal data and consumer law. In this sense, they use certain strategies to manipulate user behavior.

Given the impacts that dark patterns can have on the protection of personal data, the European Data Protection Board (EDPB) issued Guide No. 3/2022 in March 2022. Under the terms of the definition presented by the Guide, dark patterns can be understood as “user interfaces and experiences implemented on social media platforms that lead users to make unintended, unwilling and potentially harmful decisions regarding the processing of their personal data”.

From such a perspective, the Guide aims to present recommendations so that web designers and internet users in the cybernetic environment can analyze and avoid the implementation of forms of dark patterns that may violate personal data protection laws.

In addition, six types of dark patterns were enumerated, namely: (i) “Overloading”, understood by exposing users to a high volume of information and requests, aiming at inducing them to share more data or, involuntarily, allowing the processing of personal data against their interests; (ii) “Skipping”, which is revealed in the structuring of the interface in such a way that users forget or do not think about all or some of the data protection aspects; (iii) “Stirring”, understood as manipulating the choices that the individual would make by appealing to their emotions or using visual “nudges”; (iv) “Hindering”, understood as the imposition of digital barriers to consumers, in order to make it difficult or impossible to complete the process of managing the data collected and processed by a particular company; (v) “Fickle”, which is the projection of an unstable and inconsistent interface, in order to make it difficult for users to navigate the various data protection control mechanisms and understand the purpose of the data processing; (vi) “Left in the dark”, which is the design of an interface so as to hide information or data protection control tools, or make users unsure about how their data is handled and what kind of control they can have over it to safeguard their rights.



## Guernsey DPA publishes a guide for businesses about employee privacy obligations

The Guernsey Data Protection Authority, in the last week of August, released on its official channels a guide dealing with employers' obligations when handling personal data, as well as the applicable principles in the context of the employment relationship.

The release comes in a context of growing complexity in employment relationships, with ever-increasing processing of personal data. According to the guide, it is important to pay attention to sensitive personal data collected in the context of the employment relationship, such as employee's ethnic origin and sexual orientation, since such data require a higher level of security.

In addition, the guide highlights the importance of being bound by personal data processing principles such as the adequacy and the purpose of the processing, the necessity of collecting such personal data, and the confidentiality of such personal data vis-à-vis third parties.

## ICO publishes a guide for small businesses to respond to data protection complaints

In August 2022, the Information Commissioner's Office (ICO) – the UK's independent authority responsible for upholding the public interest in data privacy matters – published a guide to advise small businesses on how to proceed when they receive a request regarding the protection of personal data.

Sometimes employees, customers, contractors, or other data subjects may not be satisfied with how a company has processed their personal data, so the guide provides guidance on the appropriate steps to be taken in such situations that will help maintain the company's reputation for being concerned about personal data protection.

The guide outlines six steps to accomplish this: acknowledging the receipt of the request, understanding the specific problem related to the request, providing regular updates to the data subject, recording the steps and actions taken in response to the request, and formally responding to the data subject with the findings of the investigation or resolution of the problem, and finally, reviewing the lessons learned from the request received to prevent future requests.

Besides detailing the actions to be taken at each step, the ICO also recommends that the communication with the data subject should always be in clear, specific, and direct language to avoid potential misunderstandings.

By following all these steps in replying to a data subject request, you will demonstrate a concern for solving the problem, which helps building greater trust from customers, employees, contractors, and other data subjects.

## Foreign nationals now have the right to access personal data processed by Canadian institutions

As of July 13, 2022, foreign nationals outside Canada, per the Privacy Act, will have the right to access personal data being processed by federal government institutions. The extension of the right was given by Extension Order No. 3 to the Canadian Privacy Act.

Until then, foreign nationals outside Canada were dependent on a service provided by a third party who would act as an agent and make the access request on behalf of the foreign data subject. Now, the request can be made by the data subject himself.

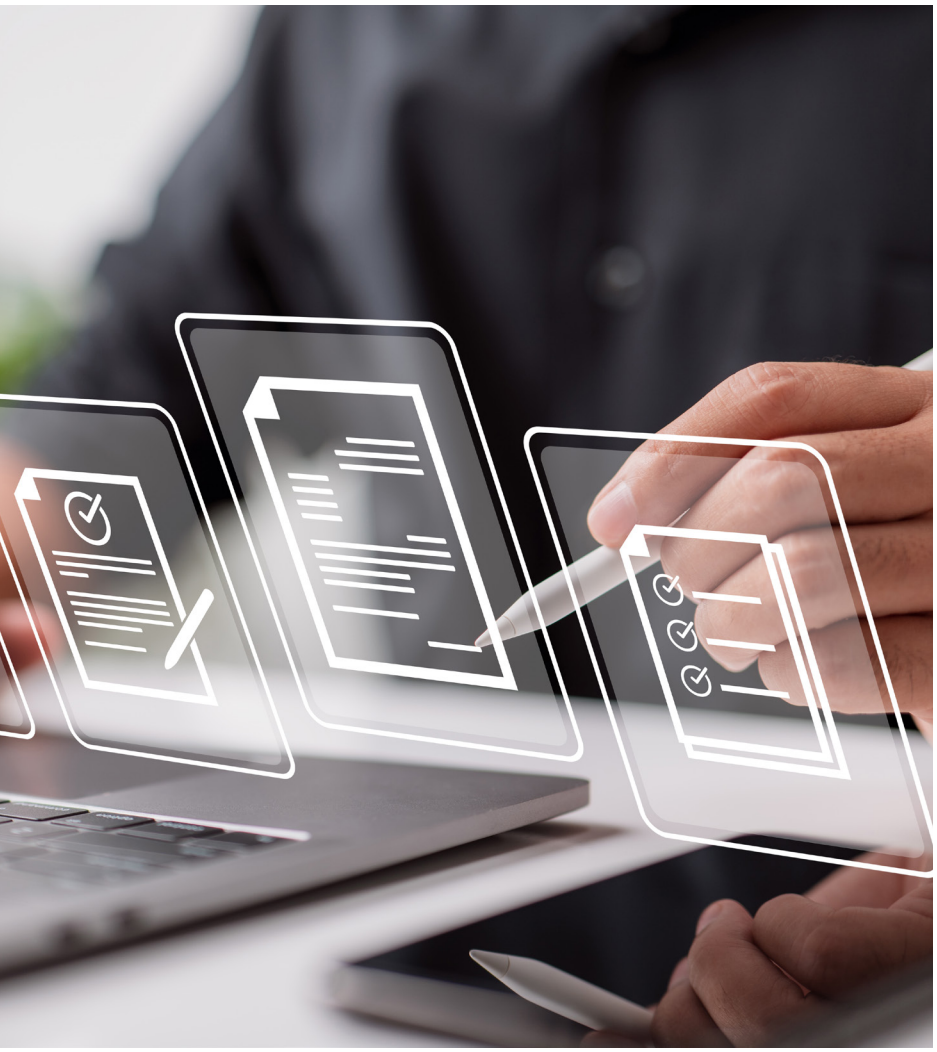
Additionally, the Extension Order has also ensured that foreign nationals can submit complaints to the Canadian Privacy Commissioner if they feel that their access to personal data is being denied, delayed, or that the information is inaccurate.

## Supervisory Authorities of the Baltic States launch a coordinated inspection of the compliance of personal data processing in the field of short-term vehicle rental

In September 2021, during a meeting of Supervisory Authorities (SA) for the protection of personal data of the Baltic States, it was concluded that closer cooperation between supervisory authorities will contribute to more efficient supervision of data processing in the Baltic States. Because of this, the Baltic States' SA launched a coordinated preventive supervision on the compliance of personal data processing in the field of short-term vehicle rental.

This initiative emerged to develop recommendations to improve data protection in this market segment, proactively addressing potential threats to citizens' personal data. In this sense, the SA agreed that inspection will be exercised over companies that offer short-term vehicle rental, whose main customers are natural persons.

This way, all companies in the sector that offer their services in the Baltic States will be monitored. With regard to its decision-making independence, each SA may extend the scope of the supervision to the activities of enterprises who are also active in only one Member State.



## TJSP decides that proof of damage is required for civil liability of a company responsible for leakage of consumer data

The 35th Chamber of Private Law of the Court of Justice of São Paulo dismissed an appeal considering that the Plaintiff had not proven the moral damage resulting from the leakage of personal data by the electric utility company. The reporting judge also understood that the leaked data were not sensitive and did not compromise the dignity of the Plaintiff.

The consumer had triggered the Court to request compensation for alleged moral damages, claiming that the leakage of her data led her to experience numerous problems, such as receiving unwanted messages and advertisements on her mobile phone. The first-degree judgment dismissed the claim in a decision that was upheld by the court. According to the Court, "once the occurrence of moral damage is ruled out, the dismissal of the claim is a measure of rigor".

The final judgment by the Court established that, despite the strict liability of the electric utility company regarding the processing of data (art. 42 of the LGPD), the analysis of the existence of damage is required.

## Superior Electoral Court decides that candidate data must be kept public

The Superior Electoral Court's plenary decided to keep public the data regarding candidates for the 2022 elections. Keeping only data such as an address, e-mail, and personal phone numbers, the collegiate also understood that the declaration of assets must be made public.

The discussion on the subject began after a request made by Luciano Reginaldo Fulcro, elected as an alternate councilman for the City of Guarulhos. The Court accepted the request for his data to be deleted from the platform due to threats he suffered during the elections.

Minister Alexandre de Moraes, however, in a session held in August, voted in favor of the publication of data related to candidates, arguing that the Brazilian General Data Protection Law is a general law, while the Electoral Legislation is a specific law, not subject to the restrictions of the general law.

Justice Edson Fachin, the presiding judge in the case, had previously voted to maintain transparency as a rule, limiting it only to data regarding the intimacy and privacy of candidates. Thus, he defended the maintenance of the platform as a form of social control, which allows society to monitor the candidacies of their representatives.

# The Judgment on the constitutionality of the Decree regulating the disclosure of data by public administration has been started

**Earlier this month, the Supreme Court initiated the judgment on the constitutionality of Decree No. 10,046/2019. This Decree regulates data disclosure within the federal public administration and establishes the Citizen Base Registry and the Central Data Governance Committee.**

**The Decree is the subject of two lawsuits (ADI 6.649 and ADPF 695), which, in a trial that took place on September 15, 2022, were partially upheld to give the Decree an interpretation in accordance with the provisions of the Federal Constitution. The Justices of the STF understood that the Decree does not protect the rights of citizens because it allows a diffusion of sensitive data among government entities, running away from what the LGPD provides for.**

**According to the vote of Justice Gilmar Mendes, rapporteur of the actions, the sharing of data by the government should be limited to the minimum necessary, conditioned only to certain public interests that prove to be legal, necessary, and legitimate, in addition to the need for a strict supervision and control of activities undertaken by public agencies, in strict compliance with the LGDP. Furthermore, the rapporteur also established the understanding that if the guidelines of the LGPD are disobeyed, the state will be liable objectively for damages caused to individuals.**

**Furthermore, according to the rapporteur's vote, it was determined that the General Data Governance Committee should be reformulated within 60 days, since it is composed only of executive branch bodies, and should also include the participation of civil society. This was, however, a point of divergence in the vote of Justices André Mendonça and Kassio Nunes Marques, who understood that this reorganization should only occur as of December 31 of this year.**

**Justice Fachin also presented a divergent vote, holding the position that the entire decree is unconstitutional, but agreeing with the interpretation guidelines set by the rapporteur. Justices Alexandre de Moraes, Roberto Barroso, Luiz Fux, Dias Toffoli, Carmen Lúcia, Ricardo Lewandowski, and Rosa Weber followed Gilmar Mendes in their votes.**

# Supreme Court discusses whether the exposure of criminal or labor proceedings through search for personal data on the Internet is considered a violation of the LGPD

The Court of Justice of the State of Rio Grande do Sul dismissed a case on personal data, understanding that it is lawful to present public proceedings through the search for personal data of those involved on the Internet. The Defendant appealed to the Supreme Court, for the decision taken to be signed nationwide.

However, the Attorney General of the Republic, Augusto Aras, understands that the appeal should not be provided, because the unrestricted disclosure of information about labor and criminal actions in the virtual environment, from research with personal data, violates the General Data Protection Law: "The processing of publicly accessible personal data by data processing agents to allow wide publicization and consultation by name of the parties of information from labor and criminal proceedings exceed the authorization of data processing by the LGPD, given the lack of justification based on a legitimate and specific purpose in concrete and the violation of the rights of the data subject."

According to Aras, this is because the public consultation of labor and criminal actions is only allowed, in the system of the courts, from the number of the process, not being possible to identify the case with personal data of those involved.

The Attorney General also claims that this extensive information disclosed can cause damages to those involved, who will have their image linked to labor and criminal proceedings, also violating the right to privacy, intimacy, and data protection. Finally, he understands that those who irregularly disclose personal data should indemnify the victim in case of possible damages. The case still hangs from trial by the Supreme Court and is being dealt with under the general repercussion system, under Theme 1141 (ARE 1307386).

# Secretariats of the State of Pernambuco were ordered by MPPE to adapt to the LGPD

The Public Prosecutor's Office of Pernambuco has identified the possibility that the State Secretariat of Social Development, Children, and Youth may have violated the right to the protection of personal data. Thus, the Public Prosecutor's Office of Pernambuco recommended that the State Secretariats make adjustments so that the LGPD can be complied with, emphasizing that "personal data processing operations by public or private entities must be based on the foundations in the LGPD, such as respect for privacy, informational self-determination, human rights, dignity, and the exercise of citizenship by individuals, among others.

According to the recommendation published in the Electronic Official Gazette of MPPE, on September 5, 2022, the State Secretariats have ten days to manifest themselves about whether or not the recommendation is being complied with.

# Former health adviser found guilty of illegally accessing patient records

In early August, Christopher O'Brien, former health adviser of South Warwickshire NHS Foundation Trust, was found guilty of accessing, without reasonable justification and without the foundation's authorization, the personal data of 14 patients.

Coventry Magistrates' Court, responsible for hearing the former director's case, ordered him to pay compensation to 12 of the patients, totaling about £3,000. O'Brien pleaded guilty to the charges.

Patients at the hospital in Warwick, England, who were even known personally to O'Brien, said that the breach has put them off from going to their doctor, causing a situation of deep worry and anxiety.

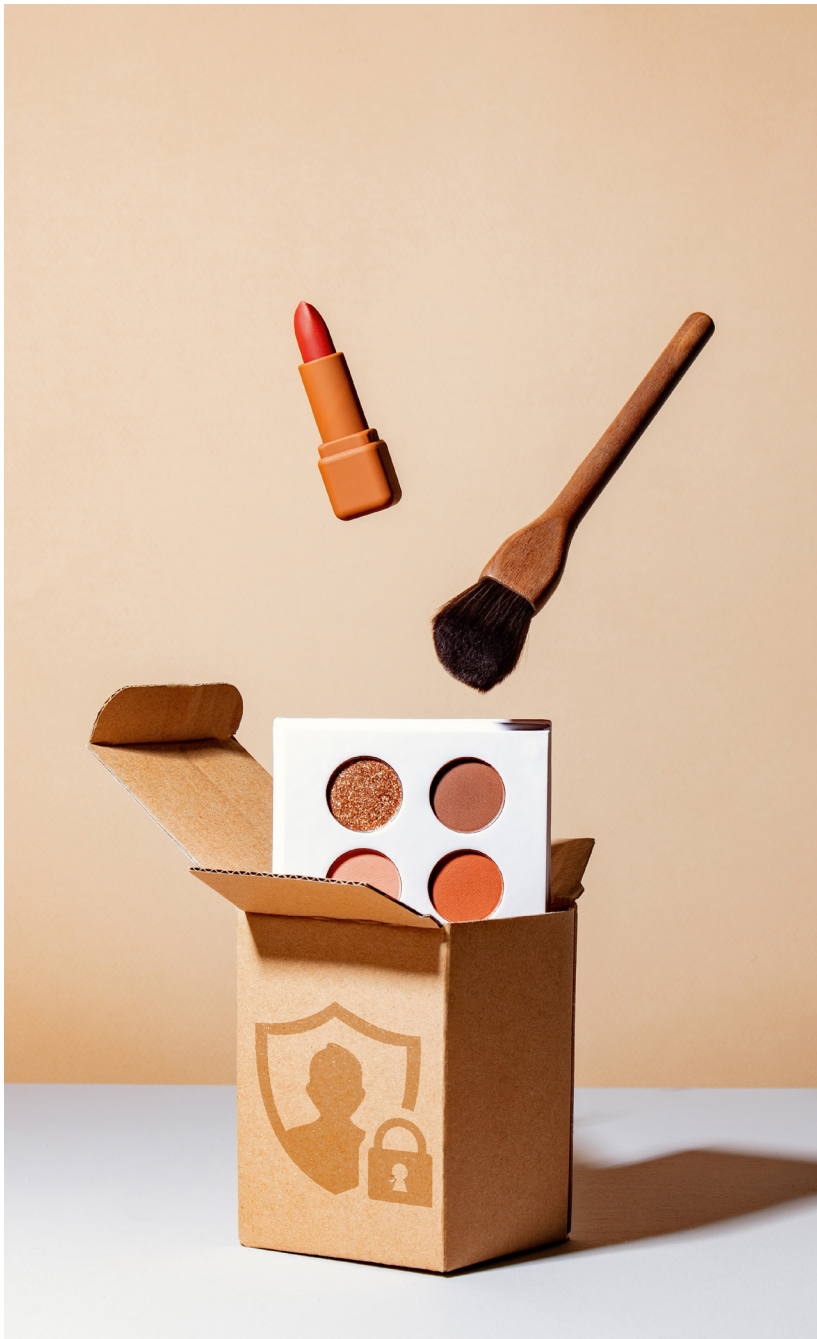
The British Data Protection Authority, ICO, through Director of Investigations Stephen Eckersley, urged organizations to reaffirm responsibilities related to data protection and information governance, particularly when dealing with sensitive personal data.

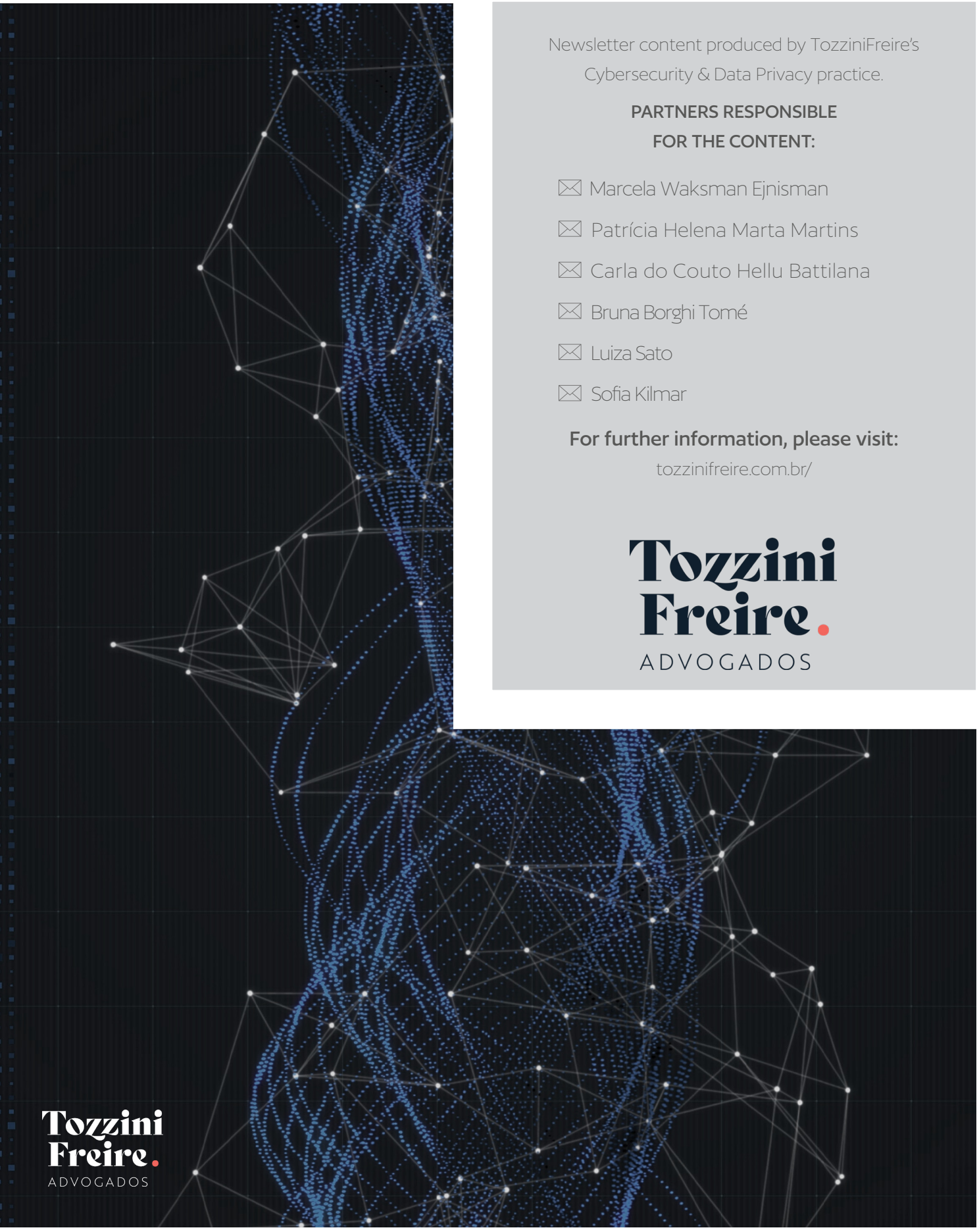
# Sephora is the first company to be fined for violating California's Consumer Privacy Act

In August 2022, California General Attorney Rob Bonta announced a settlement with French cosmetics company Sephora Inc. as the first company to be fined under the California Consumer Privacy Act (CCPA) – the "Do Not Sell" law, which provides for consumers' rights to know how companies process their data and choose not to allow them to be sold – and must pay a $1.2 million fine and meet several compliance obligations under the law.

According to information obtained from the general attorney, Sephora's violations resulted from its failure to disclose to consumers that it was selling their personal data and failed to process user requests to disable the sale of that data through privacy controls, thus violating the CCPA. Moreover, the French company failed to correct or attempt to mitigate these violations within the 30-day period currently allowed under the CCPA.

Among the obligations that Sephora will be required to comply with are: to amend its online privacy policy to clarify that it sells personal data, provide resources for consumers to opt out of having their data sold, adapt its service provider agreements to comply with the CCPA, and provide reports to the California General Attorney's office relating to the sale of personal data, the status of its relationships with service providers, and its efforts to honor the Global Privacy Control (GPC) specification.






Imagens: Shutterstock

Newsletter content produced by TozziniFreire's Cybersecurity & Data Privacy practice.

**PARTNERS RESPONSIBLE FOR THE CONTENT:**

✉ Marcela Waksman Ejnisman

✉ Patrícia Helena Marta Martins

✉ Carla do Couto Hellu Battilana

✉ Bruna Borghi Tomé

✉ Luiza Sato

✉ Sofia Kilmar

**For further information, please visit:**

tozzinifreire.com.br/

Tozzini Freire. ADVOGADOS