Draft of Regulation on Reporting Information Security Incidents

May, 2023

TAUIL | CHEQUER
MAYER | BROWN

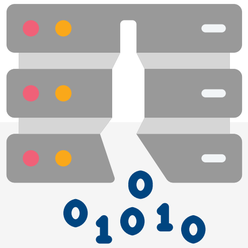
The Brazilian Data Protection Authority (ANPD) released the draft of a resolution defining the information security incident reporting procedures before the ANPD and the data subjects, as required under Article 48 of the General Data Protection Law (LGPD). The draft of the Regulation on Reporting Information Security Incidents is open to public comment until May 31, 2023 and would apply to all reports already provided to the ANPD so far.

The highlights of the draft include:

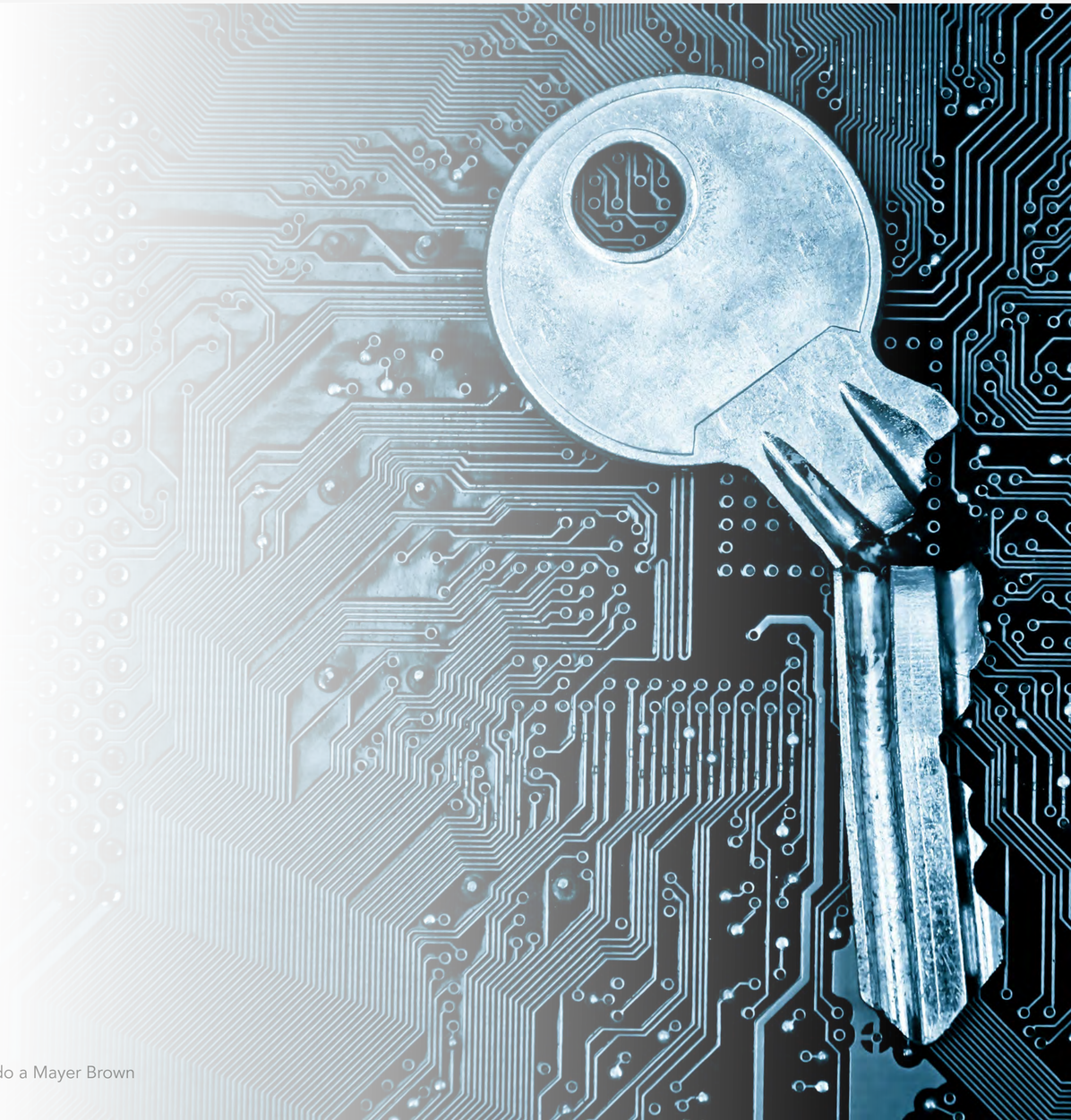
- Incident
- Triggers for reporting
- Decision not to report to the ANPD
- Deadline to report both the ANPD and the data subjects
- Main information that must be provided to the ANPD
- Main information that must be provided to the affected data subjects
- ANPD's entitlements after the report
- Controller's representation before the ANPD
- Confidentiality on the information provided to the ANPD
- Information security incidents records

INCIDENT

TAUIL | CHEQUER
MAYER | BROWN



Any **confirmed** adverse event that affects confidentiality, integrity, availability and/or authenticity of personal data.



TRIGGERS FOR REPORTING

TAUIL | CHEQUER
MAYER | BROWN

If an incident **puts, or is likely to put**, the affected data subjects at risk; or to cause a significant damage to them (Article 48 LGPD). These factors include:

When the incident significantly affect the interests or fundamental rights of the data subjects, such as:

- Preventing or limiting the exercise of rights or the use of a service
- Incurring material or moral damages to the individuals:

Discrimination

Physical harm or damage

Identity theft

Harm to reputation or public image

Financial fraud

- When the incident involves, at least:

Sensitive personal data

Data from children and/or adolescents (<18 years old) and/or elderly people (>60 years old)

Financial data

Systems authentication data

Large-scale data, as defined by the ANPD

DECISION NOT TO REPORT TO THE ANPD

TAUIL | CHEQUER
MAYER | BROWN

If the ANPD becomes aware of the incident from other sources, it may determine that the controller must provide information regarding the event to the ANPD and, if applicable, may request that a formal report be sent to the ANPD.

The ANPD may impose a daily fine if the requested communication is not delivered within the timeline fixed by the ANPD.

The ANPD may set up another procedure regarding the violation of the LGPD in the absence of a submitted report.

DEADLINE TO REPORT BOTH THE ANPD AND THE DATA SUBJECTS

Three business days from the moment the party becomes aware of the incident.

It is currently unclear whether the deadline is in reference to the controller becoming aware of the incident or any third party processing personal data on its behalf.

There may be further information within 20 business days (17 business days from the first report to the ANPD).

If necessary, the deadline may be extended to 40 business days, insofar as the controller is able to justify said extension to the ANPD

The deadline is six business days for small processing agents, as regulated under Resolution CD/ANPD No. 2 of 2022.

MAIN INFORMATION THAT MUST BE PROVIDED TO THE ANPD

TAUIL | CHEQUER
MAYER | BROWN

1. Date and time the party became aware of the incident
2. Description of the incident, including the main cause, if known
3. Description of the nature and categories of affected personal data
4. Total number of data subjects whose personal data is processed by the controller
5. Total number of data subjects whose personal data is processed, as of each of the processing activities affected by the incident
6. Number of affected data subjects, highlighting those that are children, adolescents and/or elderly people, if applicable
7. Measures adopted before and after the incident, mainly those toward reverting or mitigating the effects of the incident upon the individuals
8. Risks arising from the incident, including any likely impact on the data subjects
9. Reason for not having promptly reported the incident, if applicable
10. Declaration that that the affected data subjects have been notified

MAIN INFORMATION THAT MUST BE PROVIDED TO THE AFFECTED DATA SUBJECTS

TAUIL | CHEQUER
MAYER | BROWN

Date when the party became aware of the incident	**Description of the nature and categories of affected personal data**	**Risks to and impact on the data subjects**
Measures that were adopted and that will be adopted to revert or mitigate the effects of the incident	**Contact for gathering further information**	**Data protection officer contact information**

Recommendations to the affected individuals on how to reduce the effects of the incident (not mandatory)

The communication to the individuals must be done directly and individually (phone, email, letter or electronic message), as feasible.

If it is not possible to identify each of the affected data subjects, the report must be made publicly (website, applications, social media, call center), as long as it is easily accessible for at least 6 months.

ANPD'S ENTITLEMENTS AFTER THE REPORT

TAUIL | CHEQUER
MAYER | BROWN

After the communication is delivered, the ANPD may:

1 **Request information regarding the incident, determining a specific deadline for delivery, such as:**

- Records of processing activities (ROPA) regarding the affected data
- Data Protection Impact Assessment (DPIA)

It is currently unclear whether this would be an already prepared DPIA for the affected processing activities, or if the ANPD understands that a specific DPIA should be carried out as of the incident—likely not, given the FAQ recently issued by the ANPD on DPIAs.

- An incident treatment report, defined by this regulation draft as one which contains "copies of the documents, data and information that are relevant to describe the incident and the actions adopted to treat it, such as evidence and the incident chronology, investigation methodology, tools used and security measures adopted."

2 **The ANPD may require the controller to implement to implement urgent measures to mitigate the effects of the incident or to safekeep the data subjects' rights, without allowing the controller a chance to present evidence or information about the incident**

3 **Carry out audits or inspections, or require the same to be carried out by a third party**

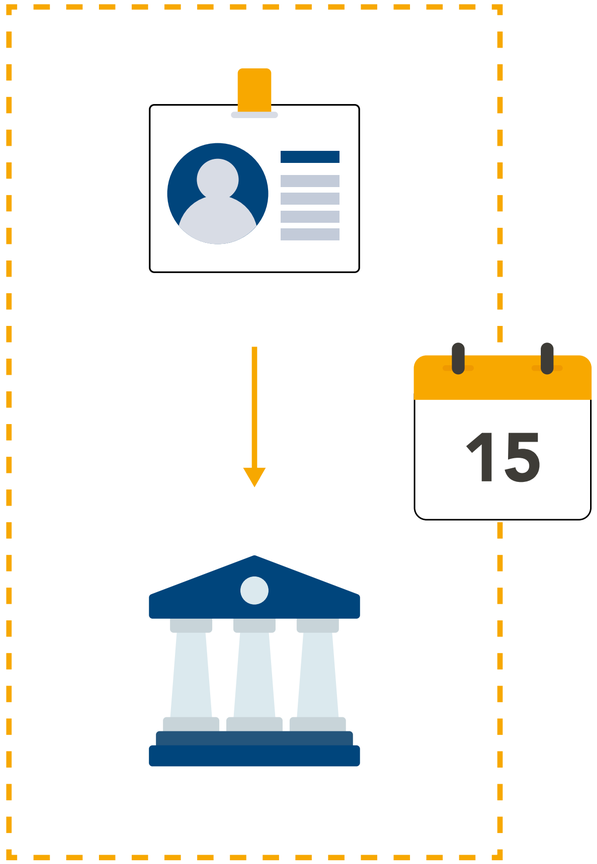
It is unclear if the ANPD is able to request that third parties carry out said audits or inspections at cost to the controller

4 **Determine that the controller disclose the incident on its website, on social media, or through newspapers, radio, TV, or any other wide-reaching media, which shall be determined in light of controller's scope of activity**

CONTROLLER'S REPRESENTATION BEFORE THE ANPD

TAUIL | CHEQUER
MAYER | BROWN

Either the Data Protection Officer's data, or the data related to a third party in charge of the report, must be provided to the ANPD. In this second scenario, any power of attorney must be provided to the ANPD within 15 business days of the first report.



CONFIDENTIALITY ON THE INFORMATION PROVIDED TO THE ANPD

TAUIL | CHEQUER
MAYER | BROWN

The controller must expressly request such confidentiality to the ANPD.

INFORMATION SECURITY INCIDENTS RECORDS

TAUIL | CHEQUER
MAYER | BROWN

As a specific accountability measure that has to be implemented by controllers (which has not been established by the LGPD), each controller must keep a record of all incidents, including those that were not reported to the ANPD and to the data subjects, for at least 5 years. Those records must contain:

- Dates when the parties became aware of the incidents
- A general description of the circumstances under which the incidents occurred
- Nature and categories of affected personal data
- Number of affected data subjects
- Assessments of the potential risks and damages to the data subjects
- Measures adopted to rectify and mitigate the effects of the incidents
- How the communications to the ANPD have been handled and who has been notified, as applicable
- Reason for not having reported incidents to the ANPD and data subjects, if applicable

Americas | Asia | Europe | Middle East

tauilchequer.com.br