CIPL submits response to Brazilian ANPD consultation on security incidents

CIPL AT 20 — SHAPING DATA POLICY FOR TOMORROW
HUNTON ANDREWS KURTH

This consultation **will inform a future regulation** by the Brazilian data protection authority (Autoridade Nacional de Proteção de Dados - ANPD) on the requirements of the Brazilian data protection law (Lei Geral de Proteção de Dados - LGPD) **concerning the notification of security incidents to the ANPD and to individuals**.

CIPL recommended that the ANPD's future regulation should:

- **Be flexible** to account for the specific contexts and varieties of any security incidents;
- **Not be prescriptive** or expect organisations to implement any specific risk assessment methodologies;
- **Provide examples** to organisations of (i) what could be potential risks and harms resulting from various types of security incidents, (ii) non-exhaustive criteria that controllers can use when assessing the level of risk involved in the security incident, and (iii) methodologies that are commonly used in the market for managing security incidents;
- **Only require notification of incidents that represent a high-risk** to individuals and result or are likely to result in material harms to them; and
- **Maintain the existing LGPD standard of an open but "reasonable" deadline** for notifying security incidents.

Download the CIPL response

EN | PT