CUATRECASAS

Intellectual Property, Media and IT / Banking, Finance and Capital Markets

Legal Flash | Portugal

November 28, 2019

Bank of Portugal's new ordinance on reporting cybersecurity incidents

Bank of Portugal's new ordinance on reporting cybersecurity incidents

On November 25, 2019, the Bank of Portugal ("BdP") issued Ordinance 21/2019, which regulates "the report mechanism of cybersecurity incidents in entities supervised by BdP and significant credit institutions in Portugal supervised by the European Central Bank" ("ECB").

BdP decided to "harmonize all report procedures and streamline communication between entities through a single point of contact that will forward, without delay, all information to the ECB and National Center for Cybersecurity ("NCC"), depending on the nature of the incident." Through this ordinance, BdP established the obligation to report all significant or serious cybersecurity incidents.

This reporting obligation applies to the following entities operating in Portugal: i) credit institutions; ii) Central Office of *Crédito Agrícola Mútuo* and Offices of *Crédito Agrícola Mútuo*; iii) investment companies; iv) payment and electronic currency institutions; and v) branches of credit institutions with overseas headquarters.

These entities must report to BdP, **no later than two hours** after detecting the incident, "all significant and serious cybersecurity incidents that have occurred or that are in progress in entities included in the supervisory perimeter, regardless of the location where their services are provided." Branches of credit institutions with overseas headquarters are not subject to the above deadline. However, they must still report all occurrences of significant and serious cybersecurity incidents that affect or may affect their business operations in the national territory.

This ordinance defines cybersecurity incidents as "all events related to information security that, with a high probability, can compromise business operations and threat information security," such as:

- having adverse effects on systems' security, applications and networks;
- jeopardizing information processed, stored and transmitted on systems, applications or networks; and
- infringing information and system security policies and user policies for applications and networks.

Once detected, institutions will analyze the material criteria in the ordinance to decide whether they are obliged to report the incident to BdP. All incidents that have or may have any effect on cybersecurity must be reported (e.g., a fire or flood in the servers' room), not only cyberattacks such as hacking or the installation of malware.

Within ten days, all entities must draft a preliminary report describing the type of incident and its impact, and, within 30 days, a final report on the incident's cause and risk-mitigating actions.

Reports to BdP are submitted via BPnet by filing a report form.

Any of the referred reports does not replace or render infective other legal reporting obligations, namely data breach notifications to the competent supervisory authority, as established by the General Regulation of Data Protection.

This ordinance enters into effect 30 business days after its publication.

Contact

Cuatrecasas, Gonçalves Pereira & Associados,
Sociedade de Advogados, SP, RL
Sociedade profissional de responsabilidade limitada

Lisboa
Praça Marquês de Pombal, 2 (e 1-8º) I 1250-160 Lisboa I Portugal
Tel. (351) 21 355 3800 I Fax (351) 21 353 2362
cuatrecasasportugal@cuatrecasas.com I www.cuatrecasas.com

Porto
Avenida da Boavista, 3265 - 5.1 I 4100-137 Porto I Portugal
Tel. (351) 22 616 6920 I Fax (351) 22 616 6949
cuatrecasasporto@cuatrecasas.com I www.cuatrecasas.com

For additional information on the contents of this document, please contact Cuatrecasas.

Information about the processing of your personal data

Data Controller: Cuatrecasas, Gonçalves Pereira & Associados, Sociedade de Advogados, SP, RL ("Cuatrecasas Portugal").
Purposes: management of the use of the website, of the applications and/or of your relationship with Cuatrecasas Portugal, including the sending of information on legislative news and events promoted by Cuatrecasas Portugal.
Legitimacy: the legitimate interest of Cuatrecasas Portugal and/or, where applicable, the consent of the data subject.
Recipients: third parties to whom Cuatrecasas Portugal is contractually or legally obliged to communicate data, as well as to companies in its group.
Rights: access, rectify, erase, oppose, request the portability of your data and/or restrict its processing, as described in the additional information.
For more detailed information on how we process your data, please go to our *data protection policy*.

If you have any questions about how we process your data, or if you do not wish to continue to receive communications from Cuatrecasas Portugal, we kindly ask you to inform us by sending a message to the following email address data.protection.officer@cuatrecasas.com.