NEWS FLASH

GPA
ADVOGADOS
LAW FIRM

PROJECTO DE INSTRUÇÃO DO BANCO DE PORTUGAL SOBRE O REPORTE DE INCIDENTES DE CIBERSEGURANÇA

Julho de 2019

Introdução

Encontra-se em consulta pública, até 19 de Agosto, um Projecto de Instrução do Banco de Portugal relativo ao reporte de incidentes de cibersegurança (Consulta Pública n.º 2/2019).

Actualmente, as entidades supervisionadas pelo Banco de Portugal devem reportar quaisquer situações com impacto nos seus resultados ou capitais próprios, incluindo eventos de índole operacional. Por outro lado, as instituições de crédito classificadas como significativas e com sede em Portugal reportam directamente ao Banco Central Europeu ("BCE") os incidentes de cibersegurança, nos termos do Regulamento-Quadro do Mecanismo Único de Supervisão.

Depois de publicada, a Instrução do Banco de Portugal agora sob consulta pública regulamentará o reporte dos incidentes de cibersegurança ocorridos em Instituições de crédito, empresas de investimento, instituições de pagamento, instituições de moeda electrónica e sucursais de instituições de crédito com sede no estrangeiro.

No que respeita às instituições de crédito significativas com sede em Portugal supervisionadas pelo BCE, o reporte dos incidentes de cibersegurança passa também a ser feito ao Banco de Portugal via Portal BP*net*, que reencaminhará automaticamente ao BCE. Adicionalmente, este reporte será enviado também ao Centro Nacional de Cibersegurança ("CNCS"), sempre que a entidade estiver classificada

como Operador de Serviços Essenciais, nos termos da Lei n.º 46/2018, de 13 de Agosto, que estabelece o regime jurídico da segurança do ciberespaço.

Finalidades da Instrução

A projectada Instrução, agora sob consulta pública, visa:

- Estabelecer o dever de comunicação de incidentes de cibersegurança significativos ou severos ocorridos em entidades supervisionadas pelo Banco de Portugal e pelo BCE;
- Harmonizar os diferentes reportes de incidentes de cibersegurança ao Banco de Portugal, BCE e CNCS, através da implementação de um modelo de reporte único; e
- Centralizar a comunicação dos incidentes de cibersegurança num ponto único de contacto, no Portal BP*net*, que reencaminhará automaticamente ao BCE e/ou CNCS quando aplicável.

Principais aspectos da Instrução

São considerados incidentes de cibersegurança *todos os eventos* (i) *que tenham um efeito adverso na segurança dos sistemas, aplicações ou redes;* (ii) *que comprometam a informação que estes sistemas, aplicações e redes processam, armazenam ou partilham; e/ou* (iii) *que infrinjam as políticas de segurança de informação e uso dos sistemas, aplicações ou redes das entidades.*

O Projecto de Instrução detalha os critérios e indicadores de materialidade para a classificação de incidentes como significativos ou severos, salientando-se, desde já, a particular abrangência destes critérios. A título de exemplo, refira-se que *devem ser classificados como significativos todos os incidentes que impliquem um processo de acompanhamento e/ou tomada de decisões por parte de instâncias internas relevantes, como sejam titulares de cargos de gestão e/ou direcção* (cfr. Art.º 4.º, n.º 6, do Projecto de Instrução).

Determina-se, ainda, que o reporte inicial deve ser feito, através do Portal BP*net*, até 2 horas após a detecção do incidente.

Mantém-se, todavia, a obrigação para os prestadores de serviços de pagamento de reporte de incidentes operacionais ou de segurança de carácter severo, em cumprimento do estabelecido do artigo 71.º do Decreto-Lei n.º 91/2018, de 12 de Novembro, que integrou no ordenamento jurídico português a disposição do artigo 96.º da DSP2, conforme Instrução do Banco de Portugal n.º 1/2019.

Mantém-se, também, o dever de notificação à Comissão Nacional de Protecção de Dados sempre que o incidente de cibersegurança resultar numa violação da protecção dos dados de pessoas singulares, ao abrigo do Regulamento Geral de Protecção de Dados.

Prevê-se que a Instrução entre em vigor no dia seguinte ao da sua publicação.