BANCO DE PORTUGAL
EUROSISTEMA

Instrução n.º 01/2019

BO n.º 1/2019 • 2019/01/15

Temas

Sistemas de Pagamentos :: Elementos de Informação

Índice

Texto da Instrução

Assunto: Reporte de incidentes de caráter severo

A Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015, relativa aos serviços de pagamento no mercado interno (DSP2), no seu artigo 96.º ("Notificação de incidentes"), consagra o dever de notificação por parte dos prestadores de serviços de pagamento (PSP), no caso da ocorrência de um incidente operacional ou de segurança de caráter severo relacionado com a prestação de serviços de pagamento.

Complementarmente, o n.º 3 do referido artigo 96.º da DSP2 determina que a Autoridade Bancária Europeia (EBA) emite Orientações relativas à classificação dos incidentes operacionais ou de segurança de caráter severo pelos PSP e de comunicação de tais incidentes à autoridade competente do Estado-Membro de origem.

Neste âmbito, a EBA emitiu as "Orientações sobre a comunicação de incidentes de caráter severo ao abrigo da DSP2" (EBA/GL/2017/10), as quais estabelecem os critérios para a classificação de incidentes operacionais ou de segurança de caráter severo e os procedimentos de comunicação desses incidentes pelos PSP às autoridades competentes. As referidas Orientações definem ainda a forma como as autoridades competentes devem avaliar a relevância dos incidentes comunicados pelos PSP e partilhar essa informação com a EBA, o Banco Central Europeu (BCE) e outras autoridades nacionais.

As supracitadas Orientações da EBA entraram em vigor em 13 de janeiro de 2018 e podem ser consultadas (na versão inglesa e portuguesa) através do seguinte link: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-major-incidents-reporting-under-psd2.

A nível nacional, o artigo 71.º do Decreto-Lei n.º 91/2018, de 12 de novembro, que transpôs a disposição relativa ao artigo 96.º da DSP2 para o ordenamento jurídico português, estabelece no seu n.º 1 que os PSP com sede em Portugal devem fazer a referida comunicação, sem demora, ao Banco de Portugal. Por seu turno, o n.º 2 do mesmo artigo determina que o Banco de Portugal deve estabelecer as normas regulamentares respeitantes à classificação, por parte dos PSP, dos referidos incidentes de caráter severo e ao conteúdo, formato, modelos e procedimentos de comunicação de tais incidentes pelos PSP.

Nestes termos, o Banco de Portugal, no uso da competência que lhe é conferida pelo artigo 14.º da sua Lei Orgânica, aprovada pela Lei n.º 5/98, de 31 de janeiro, e pelo n.º 2 do artigo 71.º do Decreto-Lei n.º 91/2018, de 12 de novembro, determina o seguinte:

I – ÂMBITO DE APLICAÇÃO E DISPOSIÇÕES GERAIS

1. Objeto

1.1. A presente instrução regulamenta o dever de comunicação, ao Banco de Portugal, dos incidentes operacionais ou de segurança de caráter 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.

1.2. Para efeito do disposto no número anterior, a presente instrução implementa as "Orientações sobre a comunicação de incidentes de caráter severo ao abrigo da DSP2" emitidas pela EBA (EBA/GL/2017/10), que estabelecem os critérios para a classificação de incidentes operacionais ou de segurança de caráter severo e os procedimentos de comunicação desses incidentes pelos PSP às autoridades competentes, substituindo o entendimento transmitido pelo Banco de Portugal através da Carta-circular n.º CC/2018/00000015, de 26 de fevereiro de 2018.

2. Destinatários

São destinatários da presente Instrução os PSP registados e autorizados pelo Banco de Portugal, ainda que operando em outros países por intermédio do exercício do direito de estabelecimento ou da livre prestação de serviços.

3. Definições

Para efeitos da presente Instrução são aplicáveis as definições constantes no Decreto-Lei n.º 91/2018 e as seguidamente indicadas:

Incidente operacional ou de segurança: Um evento único ou uma série de eventos conexos e não previstos pelo PSP, que tem, ou poderá vir a ter, um impacto adverso na integridade, disponibilidade, confidencialidade, autenticidade e/ou continuidade dos serviços relacionados com pagamentos.

Integridade: Característica que salvaguarda a exatidão e completude dos ativos (incluindo dados).

Disponibilidade: Característica que permite o acesso e a utilização dos serviços relacionados com pagamentos pelos utilizadores de serviços de pagamento.

Confidencialidade: Característica que inibe o acesso ou a divulgação de informação a indivíduos, entidades ou processos não autorizados.

Autenticidade: Característica que confirma a veracidade de uma fonte.

Continuidade: Característica necessária aos processos, tarefas e ativos de uma organização para que a prestação de serviços relacionados com pagamentos seja totalmente acessível e executada a um nível aceitável predefinido.

Serviços relacionados com pagamentos: Qualquer atividade comercial na aceção da alínea vv) do artigo 2.º do Decreto-Lei n.º 91/2018 e todas as tarefas de suporte técnico necessárias à correta prestação de serviços de pagamento.

II – REQUISITOS DE REPORTE

4. Classificação de um incidente como severo

4.1. Os PSP devem classificar como severos os incidentes operacionais ou de segurança que preencham:

4.1.1. um ou mais critérios de "nível de impacto superior", ou

4.1.2. três ou mais critérios de "nível de impacto inferior",

conforme indicado na tabela seguinte:

Critérios	Nível de impacto inferior	Nível de impacto superior
Operações afetadas	> 10 % do nível normal de operações do PSP (em termos de número de operações) **e** > 100 000 EUR	> 25 % do nível normal de operações do PSP (em termos de número de operações) **ou** > 5 milhões EUR
Utilizadores de serviços de pagamento afetados	> 5 000 **e** > 10 % dos utilizadores de serviços de pagamento do PSP	> 50 000 **ou** > 25 % dos utilizadores de serviços de pagamento do PSP
Interrupção do serviço	> 2 horas	Não aplicável
Impacto económico	Não aplicável	> Máximo (0,1 % dos fundos próprios de nível 1, 200 000 EUR) * **ou** > 5 milhões EUR

Critérios	Nível de impacto inferior	Nível de impacto superior
Encaminhamento para as instâncias superiores internas	Sim	Sim, e probabilidade de ativação do modo de crise (ou outro equivalente)
Outros PSP ou infraestruturas relevantes potencialmente afetados	Sim	Não aplicável
Impacto na reputação	Sim	Não aplicável

* Fundos próprios de nível 1, na aceção do artigo 25.º do Regulamento (UE) n.º 575/2013 do Parlamento Europeu e do Conselho, de 26 de junho, relativo aos requisitos prudenciais para as instituições de crédito e para as empresas de investimento e que altera o Regulamento (UE) n.º 648/2012.

5. Critérios / indicadores a considerar

5.1. Os PSP devem avaliar os incidentes operacionais ou de segurança de acordo com os critérios e respetivos indicadores subjacentes a seguir indicados:

5.1.1. Operações afetadas: os PSP devem determinar o valor total das operações afetadas, assim como o número de pagamentos comprometidos, em termos percentuais relativamente ao nível normal de operações de pagamento executadas pelos serviços de pagamento afetados.

5.1.2. Utilizadores de serviços de pagamentos afetados: os PSP devem determinar o número de utilizadores de serviços de pagamento afetados quer em termos absolutos, quer em termos percentuais, relativamente ao número total de utilizadores de serviços de pagamento.

5.1.3. Interrupção do serviço: os PSP devem determinar o período de tempo em que o serviço se encontrará provavelmente indisponível para os utilizadores de serviços de pagamento ou em que a ordem de pagamento, na aceção da alínea ii) do artigo 2.º do Decreto-Lei n.º 91/2018, não poderá ser executada pelo PSP.

5.1.4. Impacto económico: os PSP devem determinar os custos monetários globais do incidente e ter em conta quer os valores absolutos quer, quando pertinente, a importância relativa desses custos em relação à dimensão do PSP (ou seja, aos fundos próprios de nível 1 do PSP).

5.1.5. Encaminhamento para as instâncias superiores internas: os PSP devem determinar se o incidente em causa foi, ou provavelmente será, comunicado aos seus diretores executivos.

5.1.6. Outros PSP ou infraestruturas relevantes potencialmente afetadas: os PSP devem determinar as prováveis implicações sistémicas do incidente, nomeadamente o risco de contágio de outros PSP, infraestruturas do mercado financeiro e/ou sistemas de pagamento com cartões.

5.1.7. Impacto na reputação: os PSP devem determinar de que forma o incidente pode prejudicar a confiança dos utilizadores no próprio PSP e, de uma forma geral, no serviço em causa ou em todo o mercado.

5.2. Os PSP devem calcular o valor dos indicadores de acordo com a seguinte metodologia:

5.2.1. Operações afetadas: regra geral, os PSP devem considerar como "operações afetadas" todas as operações nacionais e transfronteiriças que tenham sido, ou possam vir a ser, direta ou indiretamente afetadas pelo incidente e, nomeadamente, as operações que não tenham sido iniciadas ou processadas, bem como as operações cujo conteúdo da mensagem de pagamento tenha sido alterado e aquelas que tenham sido ordenadas de forma fraudulenta (independentemente dos fundos terem sido recuperados ou não). Adicionalmente, os PSP devem considerar como nível normal de operações de pagamento a média diária anual das operações de pagamento nacionais e transfronteiriças executadas pelos mesmos serviços de pagamento que foram afetados pelo incidente, considerando o exercício anterior como período de referência para efeitos de cálculo. Se os PSP não considerarem este número representativo (por ex., devido à sazonalidade), devem utilizar outra medida mais representativa e transmitir ao Banco de Portugal o racional subjacente a essa abordagem no campo correspondente do relatório de reporte.

5.2.2. Utilizadores de serviços de pagamentos afetados: os PSP devem considerar como "utilizadores de serviços de pagamento afetados" todos os clientes (nacionais ou estrangeiros, consumidores ou empresas) que possuam um contrato com o PSP afetado que lhes garante o acesso ao referido serviço e que tenham sofrido ou possam vir a sofrer as consequências do incidente. Para determinar o número de utilizadores de serviços de pagamento que possam ter utilizado o serviço durante o período de ocorrência do incidente, os PSP devem recorrer a estimativas baseadas nos respetivos históricos de atividade. No caso de se tratar de um grupo, cada PSP deve apenas considerar os seus próprios utilizadores de serviços de pagamento. Se se tratar de um PSP que disponibilize serviços operacionais a terceiros, o mesmo deve considerar apenas os seus próprios utilizadores de serviços de pagamento (se tiver algum) e os PSP que usufruem desses serviços operacionais devem avaliar o incidente em relação aos seus próprios utilizadores de serviços de pagamento. Além disso, os PSP devem considerar como número total de utilizadores de serviços de pagamento o número agregado de utilizadores de serviços de pagamento nacionais e transfronteiriços contratualmente vinculados no momento do incidente (ou, em alternativa, o valor mais recente disponível) e com acesso ao serviço de pagamento afetado, independentemente

da respetiva dimensão ou de serem considerados utilizadores ativos ou passivos dos serviços em causa.

5.2.3. Interrupção do serviço: os PSP devem considerar o período de tempo em que qualquer tarefa, processo ou canal relacionado com a prestação de serviços de pagamento está, ou pode vir a estar, interrompido e que impede: i) a iniciação e/ou execução de um serviço de pagamento e/ou ii) o acesso a uma conta de pagamento. Os PSP devem contabilizar o tempo de interrupção do serviço a partir do início da interrupção, considerando quer o período de tempo em que a prestação de serviços de pagamento está disponível ao público, quer as horas de encerramento e os períodos de manutenção, quando relevante e aplicável. Caso os PSP não consigam determinar a altura em que a interrupção do serviço teve início, devem excecionalmente contabilizar a interrupção a partir do momento da sua deteção.

5.2.4. Impacto económico: os PSP devem considerar os custos direta e indiretamente relacionados com o incidente. Entre outros fatores, os PSP devem ter em conta os fundos ou ativos expropriados, os custos de substituição de *hardware* ou *software*, outros custos judiciais ou de resolução de conflitos, taxas por incumprimento de obrigações contratuais, sanções, responsabilidades externas e perdas de receitas. No que diz respeito aos custos indiretos, os PSP devem considerar apenas aqueles que já forem do conhecimento ou os que são muito prováveis de se materializar.

5.2.5. Encaminhamento para as instâncias superiores internas: os PSP devem considerar se, em resultado do impacto nos serviços relacionados com pagamentos, o Diretor Executivo de Informação (ou cargo equivalente) foi, ou provavelmente será, informado do incidente fora do âmbito de qualquer procedimento de notificação periódico e numa base continuada durante o período de ocorrência do incidente. Além disso, os PSP devem considerar se foi, ou é provável que seja, ativado o modo de crise em resultado do impacto do incidente nos serviços relacionados com pagamentos.

5.2.6. Outros PSP ou infraestruturas relevantes potencialmente afetadas: os PSP devem avaliar o impacto do incidente no mercado financeiro, incluindo as infraestruturas do mercado financeiro e/ou os sistemas de pagamento com cartões que as suportam e os outros PSP. Em particular, os PSP devem avaliar se o incidente teve, ou pode vir a ter, repercussões noutros PSP, se afetou, ou pode vir a afetar, o adequado funcionamento das infraestruturas do mercado financeiro e se comprometeu, ou pode vir a comprometer, o bom funcionamento de todo o sistema financeiro. Os PSP devem estar atentos a vários fatores, nomeadamente se o componente/*software* afetado é privado ou de acesso generalizado, se a rede comprometida é interna ou externa e se o PSP deixou, ou pode vir a deixar, de cumprir as suas obrigações nas infraestruturas do mercado financeiro às quais pertence.

5.2.7. Impacto na reputação: os PSP devem considerar o nível de visibilidade que, tanto quanto seja do seu conhecimento, o incidente obteve, ou pode vir a obter, no mercado. Os PSP devem considerar, nomeadamente, a probabilidade de o incidente poder causar danos à sociedade como um bom indicador para aferição do impacto potencial do incidente na sua reputação. Os PSP devem ter em consideração: i) se o incidente afetou algum processo com visibilidade já foi, ou se poderá ser, alvo de divulgação nos meios de comunicação social (incluindo para além dos meios tradicionais, como os jornais, também os blogues, as redes sociais, etc.), ii) se os requisitos regulamentares foram, ou podem vir, a ser incumpridos, iii) se as sanções foram, ou podem vir a ser, aplicadas ou iv) se o mesmo tipo de incidente já ocorreu anteriormente.

5.3. Os PSP devem recorrer a estimativas quando não se encontrem disponíveis dados reais para sustentar a sua avaliação sobre se um determinado limite foi, ou é provável que venha a ser, alcançado antes da resolução do incidente (por ex., tal poderá acontecer durante a fase de investigação inicial).

5.4. Os PSP devem efetuar essa avaliação durante todo o período de ocorrência do incidente, de modo a identificar eventuais alterações de estado do incidente, quer sejam no sentido do seu agravamento (de não severo para severo) ou desagravamento (de severo para não severo).

III – PROCESSO DE REPORTE

6. Canal de reporte

6.1. Os PSP devem comunicar ao Banco de Portugal os incidentes de caráter severo através do preenchimento de um relatório, em língua inglesa, no portal BP*net* (www.bportugal.net).

6.2. Para o efeito, os responsáveis pela submissão dos reportes ao Banco de Portugal devem aderir ao serviço "Sistemas de Pagamentos » Reporte de incidentes DSP2" disponibilizado no portal BP*net*.

7. Modelo de reporte

7.1. Os PSP devem recolher toda a informação relevante, preencher o relatório de incidentes, de acordo com as instruções fornecidas no manual técnico que se encontra no Portal BP*net* e utilizando para o efeito o modelo também disponível no Portal BP*net*, e submetê-lo ao Banco de Portugal, enquanto autoridade competente do Estado-Membro de origem.

7.2. Os relatórios iniciais, intercalares e finais devem ser preenchidos de forma incremental, numa base de melhor esforço, à medida que os PSP forem tomando conhecimento de mais informação no decurso das suas investigações internas.

7.3. Caso aplicável, os PSP devem ainda remeter ao Banco de Portugal, através do e-mail sp.info@bportugal.pt, uma cópia da informação fornecida (ou a fornecer) aos seus utilizadores, tal como previsto na alínea b) do n.º 1 do artigo 71.º do Decreto-lei n.º 91/2018, assim que essa informação se encontrar disponível.

7.4. Os PSP devem ainda fornecer ao Banco de Portugal toda e qualquer informação adicional, caso esteja disponível e se considere pertinente para a autoridade competente, sob a forma de um ou vários anexos remetidos para o e-mail sp.info@bportugal.pt.

7.5. Os PSP devem dar resposta a qualquer pedido de informação adicional ou de esclarecimentos sobre a documentação submetida, efetuado pelo Banco de Portugal.

7.6. Os PSP devem garantir, em permanência, a confidencialidade e a integridade da informação trocada com o Banco de Portugal.

8. Reporte inicial

8.1. Os PSP devem submeter um relatório inicial ao Banco de Portugal sempre que detetarem um incidente operacional ou de segurança de caráter severo.

8.2. Os PSP devem enviar o relatório inicial ao Banco de Portugal até 4 horas após a deteção do incidente operacional ou de segurança de caráter severo, ou, no caso da BPnet não se encontrar disponível ou operacional nesse momento, assim que se encontre novamente disponível/operacional.

8.3. Os PSP devem ainda submeter um relatório inicial ao Banco de Portugal sempre que um incidente de caráter não severo se transforme num incidente de caráter severo. Neste caso específico, os PSP devem enviar o relatório inicial ao Banco de Portugal imediatamente após a deteção da alteração de estado, ou, no caso da BPnet não se encontrar disponível ou operacional nesse momento, assim que se encontre novamente disponível/operacional.

8.4. Os PSP devem incluir, nos seus relatórios iniciais, informação de caráter geral (secção A do relatório), descrevendo algumas das características essenciais do incidente e as suas prováveis consequências, com base na informação imediatamente disponível após a sua deteção ou reclassificação. Os PSP devem recorrer a estimativas sempre que não se encontrem disponíveis dados reais. Os PSP devem também incluir, nos seus relatórios iniciais, a data da próxima atualização, que deverá ocorrer assim que possível e, em circunstância alguma, poderá exceder os 3 dias úteis.

9. Reporte intercalar

9.1. Os PSP devem submeter relatórios intercalares cada vez que considerem existir uma atualização de estado relevante e, no mínimo, na data da atualização prevista no relatório anterior (independentemente de se tratar de um relatório inicial ou intercalar).

9.2. Os PSP devem submeter ao Banco de Portugal um primeiro relatório intercalar com uma descrição mais detalhada do incidente e suas consequências (secção B do relatório). Os PSP devem igualmente produzir relatórios intercalares adicionais de forma a atualizar a informação já fornecida nas secções A e B do relatório, pelo menos sempre que tenham conhecimento de informação nova relevante ou alterações significativas desde a anterior notificação (por ex., quer quando o incidente se agrava ou desagrava, quer quando são identificadas novas causas ou tomadas novas medidas de ação para resolver o problema). Não obstante, os PSP devem elaborar um relatório intercalar sempre que tal lhes seja solicitado pelo Banco de Portugal.

9.3. À semelhança do definido para os relatórios iniciais, sempre que não se encontrem disponíveis dados reais, os PSP devem recorrer a estimativas.

9.4. Os PSP devem também incluir, em todos os relatórios intercalares, a data da próxima atualização, que deverá ocorrer assim que possível e, em circunstância alguma, poderá exceder os 3 dias úteis. Se o PSP não for capaz de cumprir a data prevista para a próxima atualização, deve contactar o Banco de Portugal para explicar os motivos do atraso, propor um novo prazo de entrega plausível (não mais do que 3 dias úteis) e enviar um novo relatório intercalar atualizando exclusivamente a informação relativa à data prevista para a próxima atualização.

9.5. Os PSP devem enviar o último relatório intercalar assim que as atividades correntes forem retomadas e a atividade comercial regresse à normalidade, informando o Banco de Portugal deste facto. Os PSP devem considerar que a atividade comercial regressou à normalidade quando as atividades/operações forem repostas para os níveis de serviço/condições definidos pelo PSP, ou estipulados por entidade externa através de um Acordo de Nível de Serviço (SLA), no que diz respeito a prazos de processamento, capacidade, requisitos de segurança, entre outras e quando deixarem de se aplicar as medidas de contingência.

9.6. No caso da atividade comercial regressar à normalidade num espaço de tempo inferior a 4 horas a contar da deteção do incidente, os PSP devem procurar submeter simultaneamente o relatório inicial e o último relatório intercalar (preenchendo as secções A e B) dentro desse prazo de 4 horas.

10. Reporte final

10.1. Os PSP devem enviar um relatório final quando efetuada a análise da causa do problema (independentemente de já terem sido implementadas medidas de mitigação ou de ter sido identificada a derradeira causa do problema) e se encontrarem disponíveis dados reais para substituir quaisquer estimativas.

10.2. Os PSP devem entregar o relatório final ao Banco de Portugal no prazo máximo de 2 semanas após o regresso à normalidade. Os PSP que necessitem de uma prorrogação do prazo (por ex., por ainda não se encontrarem disponíveis os valores reais sobre o impacto) devem contactar o Banco de Portugal antes de findo o prazo e fornecer uma justificação adequada para o atraso, bem como uma nova estimativa da data de entrega do relatório final.

10.3. No caso dos PSP conseguirem fornecer toda a informação solicitada no relatório final (secção C do relatório) no prazo de 4 horas após a deteção do incidente, devem procurar submeter, no seu relatório inicial, a informação relacionada com os relatórios inicial, último intercalar e final.

10.4. Os PSP devem procurar incluir nos seus relatórios finais toda a informação disponível, nomeadamente: i) os valores reais do impacto em vez de estimativas (bem como qualquer outra atualização necessária nas secções A e B do relatório) e ii) a secção C do relatório, que inclui a causa do problema, se já for do conhecimento, e uma síntese das medidas adotadas ou previstas adotar para resolver o problema e evitar a sua recorrência no futuro.

10.5. Os PSP devem ainda enviar um relatório final quando, em resultado de uma avaliação contínua do incidente, concluírem que um incidente anteriormente comunicado já não preenche os critérios para ser considerado severo nem é expectável que os preencha antes da resolução do incidente. Neste caso, os PSP devem enviar o relatório final assim que esta situação for detetada e, em todo o caso, na data prevista para o próximo relatório. Nesta situação em particular, em vez de preencher a secção C do relatório, os PSP devem selecionar a caixa "incidente reclassificado como não severo" e explicar os motivos que justificam o seu desagravamento.

11. Delegação do reporte

Sempre que tal seja autorizado pelo Banco de Portugal, os PSP que pretendam delegar as suas obrigações de comunicação de incidentes de caráter severo ao abrigo do artigo 71.º do Decreto-lei n.º 91/2018 a um terceiro devem informar o Banco de Portugal e assegurar o preenchimento das seguintes condições:

11.1. O contrato formal ou, quando aplicável, os acordos internos celebrados no âmbito de um grupo, subjacentes à delegação das obrigações de comunicação entre o PSP e um terceiro

definem de forma inequívoca as responsabilidades atribuídas a cada uma das partes. Em particular, devem referir claramente que, independentemente da possível delegação das obrigações de comunicação, o PSP afetado continua a ser inteiramente responsável pelo cumprimento dos requisitos definidos no artigo 71.º do Decreto-Lei n.º 91/2018, assim como pelo conteúdo da informação fornecida ao Banco de Portugal.

11.2. A delegação da obrigação de comunicação deve cumprir os requisitos de externalização de funções operacionais importantes, conforme estabelecido:

a) no artigo 71.º do Decreto-lei n.º 91/2018 relativamente às instituições de pagamento e às instituições de moeda eletrónica, aplicável *mutatis mutandis* em conformidade com o artigo 3.º da Diretiva 2009/110/CE (Diretiva da Moeda Eletrónica); ou

b) nas Orientações do Comité Europeu de Supervisão Bancária (CESB) sobre a externalização em relação a instituições de crédito.

11.3. A informação deve ser previamente submetida ao Banco de Portugal e, em todo o caso, cumprindo todos os prazos e procedimentos estabelecidos pelo Banco de Portugal.

11.4. A confidencialidade de dados sensíveis e a qualidade, consistência, integridade e fiabilidade da informação a fornecer ao Banco de Portugal é adequadamente garantida.

12. Reporte consolidado

Os PSP que desejem permitir que um terceiro designado cumpra as suas obrigações de comunicação de uma forma consolidada (nomeadamente através da apresentação de um único relatório referente a vários PSP afetados pelo mesmo incidente operacional ou de segurança de caráter severo) devem informar o Banco de Portugal, incluir a informação de contacto referente ao "PSP afetado" no modelo de relatório e assegurar que as seguintes condições são preenchidas:

12.1. Incluir esta disposição no contrato subjacente à delegação das obrigações de comunicação.

12.2. Condicionar a comunicação de forma consolidada ao facto de o incidente ter sido causado por uma perturbação dos serviços prestados por um terceiro.

12.3. Limitar a comunicação de forma consolidada aos PSP estabelecidos em Portugal.

12.4. Garantir que o terceiro avalia a materialidade do incidente relativamente a cada PSP afetado e inclui no relatório consolidado apenas os prestadores para quem o incidente seja considerado de caráter severo. Em caso de dúvida, garantir que o PSP é incluído no relatório consolidado sempre que não existam evidências de que não deva ser incluído.

12.5. Garantir que, sempre que existam campos no modelo de relatório em que não seja possível fornecer uma resposta comum (por ex., secções B2, B4 ou C3), o terceiro procede: i) ou ao preenchimento individual para cada PSP afetado, identificando especificamente cada

prestador a que a informação diz respeito, ii) ou à utilização de intervalos, nos campos que permitam essa opção, representando os valores mínimos e máximos observados ou estimados dos diversos PSP.

12.6. Os PSP devem assegurar-se de que o terceiro os mantém permanentemente a par de toda a informação relevante relativa ao incidente e de todas as interações que a mesma possa ter com o Banco de Portugal, bem como do teor de tais interações, mas apenas na medida em que tal não implique uma quebra de confidencialidade relativamente a informação relacionada com outros PSP.

IV – DISPOSIÇÕES FINAIS

13. Entrada em vigor

A presente instrução entra em vigor no dia da sua publicação.