

**RESOLUÇÃO DE LITÍGIOS**

Subcontratação de prestadores de serviços de computação em nuvem

Circular n.º 3/2021

A Autoridade Europeia dos Seguros e Pensões Complementares de Reforma (“EIOPA”) tem como atribuição¹ emitir orientações e recomendações, dirigidas às autoridades de supervisão dos Estados-Membros, sobre como as empresas de seguros e resseguros devem aplicar a Diretiva Solvência II², por forma a (i) estabelecer práticas de supervisão consistentes, eficientes e eficazes e (ii) assegurar a aplicação comum, uniforme e coerente do direito da União.

Neste contexto, a 6 de fevereiro de 2020, foram publicadas as orientações da EIOPA relativas à subcontratação de prestadores de serviços de computação em nuvem³ (“Orientações”), cuja aplicação se iniciou a 1 de janeiro de 2021 a todos os acordos de subcontratação em causa celebrados ou alterados a partir dessa data e cuja implementação se pretende até ao dia 31 de dezembro de 2022.

Por sua vez, a 11 de maio de 2021, a ASF⁴ emitiu a Circular n.º 3/2021, mediante a qual comunicou ser sua intenção lançar uma consulta pública relativa ao projeto de Norma Regulamentar que incorporará as referidas Orientações, bem como a condução de questionários de diagnóstico ao mercado segurador nacional, que permitam identificar a experiência das empresas de seguros no que concerne às inovações digitais em apreço.

Independentemente dos avanços ao nível da regulação pela ASF e do momento em que venha a ser publicada a mencionada Norma Regulamentar, torna-se premente uma breve análise às Orientações já publicadas pela EIOPA, que têm vindo a preocupar as empresas de seguros no que respeita à adaptação que o regulador nacional irá exigir quanto aos processos de subcontratação.

"Foram publicadas as orientações da EIOPA relativas à subcontratação de prestadores de serviços de computação em nuvem."

Margarida Ferraz
de Oliveira

Paula Bento Neto

Equipa de Resolução
de Litígios

1 Por força do artigo 16.º do Regulamento (UE) n.º 1094/2010, do Parlamento Europeu e do Conselho, de 24 de novembro de 2010.

2 Diretiva n.º 2009/138/CE do Parlamento Europeu e do Conselho, de 25 de Novembro de 2009.

3 EIOPA-BoS-20-002, disponível [aqui](#).

4 Autoridade de Supervisão de Seguros e Fundos de Pensões.

"As empresas de seguros terão de rever as atuais disposições de subcontratação relacionadas com funções ou atividades operacionais essenciais ou importantes e alterá-las em conformidade com as Orientações."

1. Âmbito de aplicação

As Orientações aplicam-se aos *“serviços fornecidos através de computação em nuvem, ou seja, um modelo que oferece um acesso em rede em qualquer local, prático e a pedido a um conjunto partilhado de recursos informáticos configuráveis (por exemplo, redes, servidores, sistemas de armazenamento, aplicações e serviços) que podem ser rapidamente disponibilizados e libertados com um esforço mínimo de gestão ou de interação com o fornecedor de serviços”*⁵.

No entanto, para que sejam aplicáveis as Orientações, terá de estar em causa uma subcontratação para efeitos da Diretiva Solvência II: *“qualquer tipo de acordo entre uma empresa de seguros ou de resseguros e um prestador de serviços, quer se trate de uma entidade supervisionada ou não, nos termos do qual o prestador de serviços realiza, directamente ou por sub-subcontratação, um processo, serviço ou actividade que de outra forma seria realizada pela própria empresa de seguros ou de resseguros”*⁶.

As empresas de seguros terão de rever as atuais disposições de subcontratação relacionadas com funções ou atividades operacionais essenciais ou importantes e alterá-las em conformidade com as Orientações. Se até 31 de dezembro de 2022 esta revisão não estiver concluída, as empresas de seguros deverão informar a ASF desse facto, incluindo das medidas previstas para concluir a revisão e eventual estratégia de saída de tais acordos.

2. Os princípios gerais de governação para a subcontratação de serviços em nuvem⁷

Primeiramente, requer-se que o órgão de administração, direção ou supervisão da empresa de seguros assegure que a decisão de subcontratação destes serviços seja tomada com base numa avaliação de risco exaustiva, incluindo uma avaliação global de todas as fragilidades que à subcontratação possam estar inerentes⁸.

Quando se trate da subcontratação de funções ou atividades operacionais essenciais, a empresa de seguros deverá, quando relevante, contemplar as alterações que a subcontratação implicar no seu perfil de risco e na sua avaliação interna do risco e da solvência.

5 Cfr. definição de “Serviços de computação em nuvem”, parágrafo 9 das Orientações.

6 Cfr. artigo 13.º, n.º 28, da Diretiva Solvência II.

7 Cfr. Orientação 2 das Orientações.

8 Sem prejuízo do previsto no artigo 274.º, n.º3 do Regulamento Delegado (EU) n.º 2015/35 da Comissão, de 10 de outubro de 2014 (“Regulamento Delegado”).

Ademais, na utilização de serviços de computação em nuvem, as empresas de seguros devem atender às suas estratégias já definidas e ser com elas coerentes, nomeadamente com as estratégias de tecnologias da informação e comunicação (“TIC”), de segurança da informação ou de gestão operacional de riscos, e ainda com as políticas e processos internos – devendo estes ser atualizados, se necessário.

3. Atualização da política de subcontratação

No respeitante à atualização da política de subcontratação, a EIOPA quis certificar-se que, aquando da subcontratação de prestadores de serviços de computação em nuvem, a empresa de seguros detém a sua política de subcontratação (e restantes políticas internas que sejam relevantes) atualizada, de acordo com as especificidades dos serviços em nuvem contratados, nomeadamente nas seguintes matérias:

- i) atribuições e responsabilidades das funções da empresa de seguros envolvidas na subcontratação;
- ii) processos e procedimentos de prestação de informação exigidos para a aprovação, execução, gestão e renovação dos acordos de subcontratação;
- iii) supervisão dos serviços em nuvem proporcional à natureza, escala e complexidade dos riscos associados aos serviços prestados;
- iv) requisitos contratuais, conforme descritos na Orientação 10, para a subcontratação de serviços relacionados com funções operacionais essenciais ou importantes;
- v) requisitos de documentação e notificação escrita à ASF da subcontratação de serviços relacionados com funções operacionais essenciais ou importantes; e, por fim,
- vi) quanto a cada acordo de subcontratação de funções ou atividades operacionais essenciais ou importantes, definição de uma «*estratégia de saída*» documentada.

"A EIOPA quis certificar-se que, aquando da subcontratação de prestadores de serviços de computação em nuvem, a empresa de seguros detém a sua política de subcontratação atualizada."

4. A notificação por escrito à ASF⁹

Os requisitos de notificação por escrito estabelecidos no artigo 49.º, n.º 3, da Diretiva Solvência II e especificados nas Orientações da EIOPA sobre o sistema de governação são aplicáveis a todas as subcontratações de funções e atividades operacionais essenciais ou importantes a prestadores de serviços de computação em nuvem. Caso uma função ou atividade operacional subcontratada e classificada anteriormente como não essencial ou não importante venha a tornar-se essencial ou importante, a empresa deve notificar a ASF dessa mesma alteração.

A EIOPA define, para o efeito, qual deverá ser o conteúdo mínimo da notificação por escrito ao regulador nacional.

⁹ Cfr. Orientação 4 das Orientações.

5. Requisitos de documentação

A empresa de seguros deve manter um registo das informações sobre os acordos de subcontratação de serviços de computação em nuvem que estejam em vigor, e manter os registos relativos aos acordos terminados durante um período adequado e de acordo com a legislação nacional.

A EIOPA define, para a subcontratação de serviços relacionados com funções operacionais essenciais, qual deverá ser o conteúdo mínimo dos respetivos registos.

6. Avaliação das funções e atividades operacionais essenciais

Antes de celebrar qualquer acordo de subcontratação, a empresa deve avaliar se o acordo de subcontratação diz respeito a uma função ou atividade operacional que seja essencial ou importante, ou se o pode vir a ser no futuro. Por outro lado, o carácter de essencialidade ou importância deve, igualmente, ser reavaliado se a natureza, a escala ou a complexidade dos riscos inerentes ao acordo se alterarem.

Quando é feita esta avaliação, a empresa deve ter em conta, em conjunto com o resultado da avaliação dos riscos,

- i) o potencial impacto de qualquer perturbação significativa da função ou atividade operacional subcontratada ou da incapacidade do prestador de serviços em nuvem para prestar os serviços nos níveis de serviço acordados;
- ii) o potencial impacto do acordo de subcontratação de serviços de computação em nuvem na capacidade da empresa de gerir os riscos, cumprir a lei e realizar auditorias;
- iii) a exposição agregada da empresa ao mesmo prestador de serviços em nuvem e o potencial impacto de acordos de subcontratação cumulativos na mesma área de atividade;
- iv) a dimensão e a complexidade de qualquer área de atividade afetada pelo acordo de subcontratação;
- v) a capacidade para transferir o acordo de subcontratação proposto para outro prestador de serviços de computação em nuvem, se necessário; e
- vi) a proteção de dados pessoais e não pessoais e o potencial impacto, para a empresa, tomadores de seguros ou outros titulares de dados relevantes, de uma violação da confidencialidade ou da incapacidade de assegurar a disponibilidade e a integridade dos dados¹⁰.

"A empresa deve ter em conta, em conjunto com o resultado da avaliação dos riscos, a dimensão e a complexidade de qualquer área de atividade afetada pelo acordo de subcontratação."

¹⁰ Conforme previsto no Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

7. Avaliação dos riscos

Antes de celebrar qualquer acordo com prestadores de serviço de computação em nuvem, a empresa de seguros deve identificar e avaliar todos os riscos relevantes, em particular, os riscos operacionais e reputacionais.

No caso de se tratar de uma função ou atividade operacional essencial ou importante, as empresas devem ter em conta,

- i) os benefícios e custos esperados do acordo de subcontratação, incluindo a ponderação de quaisquer riscos significativos que possam ser reduzidos; e
- ii) os riscos jurídicos, das TIC, de conformidade e de reputação, assim como as limitações de supervisão relacionadas com o serviço.

Se, após a celebração do acordo, a empresa de seguros tomar conhecimento de deficiências graves ou alterações significativas nos serviços prestados ou na situação do prestador, a avaliação de riscos deve ser revista ou novamente realizada.

8. Due Diligence em relação ao prestador de serviços

A empresa de seguros deve cumprir a devida diligência em relação ao prestador de serviços de computação em nuvem e certificar-se de que este é adequado à luz da sua política de subcontratação.

Caso a empresa celebre um segundo acordo com um prestador de serviços em nuvem que já tenha sido avaliado, deve determinar, em função do risco, se é necessário proceder a uma segunda avaliação em cumprimento do dever de «*due diligence*».

Em caso de descoberta de uma deficiência grave ou alteração significativa no serviço prestado ou relativa ao prestador, a empresa de seguros deve rever ou até repetir o exercício de *due diligence*.

Perante a subcontratação de funções operacionais essenciais ou importantes, a diligência devida deverá incluir uma avaliação da adequação do prestador de serviços em nuvem, por exemplo, quanto às suas competências, infraestruturas, situação financeira, estatuto empresarial e legal, o que pode ser comprovado com base em certificações internacionais, relatórios de auditoria de terceiros reconhecidos ou relatórios de auditoria interna.

"Em caso de descoberta de uma deficiência grave ou alteração significativa no serviço prestado ou relativa ao prestador, a empresa de seguros deve rever ou até repetir o exercício de *due diligence*."

9. Notas finais

As Orientações preveem ainda, quanto aos acordos de subcontratação em concreto, (i) requisitos contratuais, como a celebração de acordo escrito, (ii) direitos de acesso e auditoria que o prestador deve garantir à empresa de seguros, (iii) garantias quanto à segurança dos dados e dos sistemas e, ainda, (iv) direitos de rescisão e estratégias de saída.

É crucial, por isso, que as autoridades nacionais competentes em cada Estado-Membro confirmem perante a EIOPA se pretendem adotar no seu ordenamento jurídico as Orientações e de que forma o pretendem fazer, incorporando-as de forma adequada no quadro regulamentar ou de supervisão.

Na resenha das medidas introduzidas pelas Orientações, conclui-se que as empresas e as autoridades competentes deverão, na aplicação, cumprimento e fiscalização das Orientações, ter em conta o princípio da proporcionalidade¹¹ e o carácter essencial ou importante do serviço subcontratado. ■

"As Orientações preveem ainda, quanto aos acordos de subcontratação em concreto, direitos de acesso e auditoria que o prestador deve garantir à empresa de seguros."

¹¹ Cfr. Artigo 29.º, n.º 3 da Diretiva Solvência II.