EIOPA-BoS-20-002

Orientações relativas à subcontratação a prestadores de serviços de computação em nuvem

Índice

Introdução

1. Nos termos do artigo 16.º do Regulamento (UE) n.º 1094/2010[1], a EIOPA emite orientações às empresas de seguros e de resseguros sobre a forma como as disposições relativas à subcontratação estabelecidas pela Diretiva 2009/138/CE[2] («Diretiva Solvência II») e pelo Regulamento Delegado (UE) n.º 2015/35 da Comissão[3] («Regulamento Delegado») devem ser aplicadas à subcontratação a prestadores de serviços de computação em nuvem.
2. As presentes orientações baseiam-se nos artigos 13.º, n.º 28, 38.º e 49.º da Diretiva Solvência II e no artigo 274.º do Regulamento Delegado. Baseiam-se ainda nas Orientações da EIOPA sobre o sistema de governação (EIOPA-BoS-14/253).
3. As presentes orientações destinam-se às autoridades competentes estabelecendo diretrizes sobre a forma como as empresas de seguros e de resseguros (coletivamente designadas por «empresas») devem aplicar os requisitos de subcontratação previstos nos atos jurídicos acima referidos no contexto da subcontratação a prestadores de serviços de computação em nuvem.
4. As Orientações aplicam-se a empresas individuais e *mutatis mutandis* a grupos[4].

   As entidades sujeitas a outros requisitos setoriais e que fazem parte de um grupo não são contempladas pelas presentes orientações a nível individual, uma vez que devem cumprir os requisitos setoriais específicos que lhes são aplicáveis, bem como as orientações relevantes emitidas pela Autoridade Europeia dos Valores Mobiliários e dos Mercados e pela Autoridade Bancária Europeia.
5. No caso da contratação e subcontratação intragrupo de serviços de computação em nuvem, as presentes orientações devem ser aplicadas em conjunto com as disposições relativas à subcontratação intragrupo enunciadas nas Orientações da EIOPA sobre o sistema de governação.
6. As empresas e as autoridades competentes deverão, no cumprimento ou na fiscalização do cumprimento das presentes orientações, ter em conta o princípio da proporcionalidade[5] e o caráter essencial ou a importância do serviço subcontratado a prestadores de serviços de computação em nuvem. O princípio da proporcionalidade deverá assegurar que os sistemas de governação, incluindo os relacionados com a subcontratação a prestadores de serviços de computação em nuvem, sejam proporcionais à natureza, escala e complexidade dos riscos inerentes.
7. As presentes Orientações devem ser interpretadas em conjugação com e sem prejuízo das Orientações da EIOPA sobre o sistema de governação e das obrigações regulamentares enunciadas no ponto 1.

Definições

8. Se não estiverem definidos nas presentes Orientações, os termos utilizados têm a aceção que lhes é dada nos atos jurídicos mencionados na introdução.

---

[1] Regulamento (UE) n.º 1094/2010 do Parlamento Europeu e do Conselho, de 24 de novembro de 2010, que cria uma Autoridade Europeia de Supervisão (Autoridade Europeia dos Seguros e Pensões Complementares de Reforma), altera a Decisão n.º 716/2009/CE e revoga a Decisão 2009/79/CE da Comissão (JO L 331 de 15.12.2010, p. 48).

[2] Diretiva 2009/138/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, relativa ao acesso à atividade de seguros e resseguros e ao seu exercício (Solvência II) (JO L 335 de 17.12.2009, p. 1).

[3] Regulamento Delegado (UE) 2015/35 da Comissão, de 10 de outubro de 2014, que completa a Diretiva 2009/138/CE do Parlamento Europeu e do Conselho relativa ao acesso à atividade de seguros e resseguros e ao seu exercício (Solvência II) (JO L 12 de 17.1.2015, p. 1).

[4] Artigo 212.º, n.º 1, da Diretiva Solvência II.

[5] Artigo 29.º, n.º 3, da Diretiva Solvência II.

9. Além disso, para efeitos das presentes Orientações, aplicam-se as seguintes definições:

Prestador de serviços	Uma entidade terceira que desempenha, no todo ou em parte, uma atividade, um processo ou um serviço ao abrigo de um acordo de subcontratação.
Prestador de serviços de computação em nuvem	Um prestador de serviços, tal como definido anteriormente, responsável pela prestação de serviços de computação em nuvem ao abrigo de um acordo de subcontratação.
Serviços de computação em nuvem	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.
Nuvem pública	Infraestrutura em nuvem disponível para utilização em sistema aberto pelo público em geral.
Nuvem privada	Uma infraestrutura em nuvem disponível para utilização exclusiva por uma única empresa.
Nuvem comunitária	Uma infraestrutura em nuvem disponível para utilização exclusiva por uma comunidade específica de empresas, incluindo várias empresas de um único grupo.
Nuvem híbrida	Uma infraestrutura em nuvem composta por duas ou mais infraestruturas em nuvem distintas.

Data de aplicação

10. As presentes Orientações aplicam-se a partir de 1 de janeiro de 2021 a todos os acordos de subcontratação de nuvens celebrados ou alterados a partir dessa data.

11. As empresas devem rever e alterar em conformidade as atuais disposições de subcontratação relacionadas com funções ou atividades operacionais essenciais ou importantes («critical or important operational functions or activities»), a fim de garantir o cumprimento das presentes orientações até 31 de dezembro de 2022.

12. Se a revisão dos acordos de subcontratação de funções essenciais ou importantes não estiver concluída até 31 de dezembro de 2022, as empresas devem informar as suas autoridades de supervisão[6] desse facto, incluindo as medidas previstas para concluir a revisão ou a eventual estratégia de saída de tais acordos. As autoridades de supervisão podem acordar com a empresa uma prorrogação do prazo para poder concluir essa revisão, quando tal for apropriado.

13. A atualização (quando necessário) das políticas e dos processos internos da empresa deve ser efetuada até 1 de janeiro de 2021, enquanto os requisitos de documentação relativos aos acordos de subcontratação de serviços de computação em nuvem relacionados com funções ou atividades operacionais essenciais ou importantes devem ser aplicados até 31 de dezembro de 2022.

[6] Artigo 13.º, n.º 10, da Diretiva Solvência II.

Orientação 1– Serviços de computação em nuvem e subcontratação

14. A empresa deverá determinar se um acordo com um prestador de serviços de computação em nuvem é abrangido pela definição de subcontratação na aceção dada pela Diretiva Solvência II. No âmbito desta avaliação, deve ser tomado em consideração:

a. se a função ou atividade operacional (ou parte da mesma) subcontratada é realizada de forma recorrente ou contínua; e

b. se esta função ou atividade operacional (ou parte da mesma) seria normalmente abrangida pelo âmbito das funções ou atividades operacionais que seriam ou poderiam ser exercidas pela empresa no exercício das suas atividades regulares, mesmo que a empresa não tenha desempenhado anteriormente essa função ou atividade operacional.

15. Sempre que um acordo celebrado com um prestador de serviços abranja várias funções ou atividades operacionais, a empresa deve ter em conta todos os aspetos do acordo no âmbito da sua avaliação.

16. Nos casos em que a empresa subcontrata funções ou atividades operacionais a prestadores de serviços que não sejam prestadores de serviços de computação em nuvem, mas que dependam de forma significativa de infraestruturas em nuvem para prestar os seus serviços (por exemplo, quando o prestador de serviços em nuvem faz parte de uma cadeia de subcontratação), o acordo de subcontratação é abrangido pelo âmbito de aplicação das presentes orientações.

Orientação 2– Princípios gerais de governação para a subcontratação de serviços em nuvem

17. Sem prejuízo do disposto no artigo 274.º, n.º 3, do Regulamento Delegado, o órgão de administração, direção ou supervisão da empresa («OADS») deve assegurar que qualquer decisão de subcontratação de funções ou atividades operacionais essenciais ou importantes a prestadores de serviços em nuvem é tomada com base numa avaliação de risco exaustiva, incluindo todos os riscos relevantes inerentes ao acordo, como o uso de tecnologias de informação e comunicação («TIC»), a continuidade das atividades, a legalidade e conformidade, a concentração, assim como outros riscos operacionais e riscos associados à migração de dados e/ou à fase de implementação, caso aplicável.

18. Quando forem subcontratadas funções ou atividades operacionais essenciais ou importantes a prestadores de serviços de computação em nuvem, a empresa deverá, quando relevante, integrar as alterações decorrentes dos seus acordos de subcontratação no seu perfil de risco e na sua avaliação interna do risco e da solvência («AIRS»/«ORSA»).

19. A utilização de serviços de computação em nuvem deve ser coerente com as estratégias da empresa (como a estratégia de TIC, a estratégia de segurança da informação, a estratégia de gestão operacional dos riscos), assim como com as políticas e os processos internos, que devem ser atualizados, se necessário.

Orientação 3 – Atualização da política de subcontratação e respetivos documentos

20. Quando forem subcontratados prestadores de serviços de computação em nuvem, a empresa deve atualizar a sua política de subcontratação (através, por exemplo, de uma revisão dos documentos que a contêm, do aditamento de um apêndice separado ou da elaboração de novas políticas específicas), bem como as outras políticas internas relevantes (por exemplo, a política de segurança da

informação), tendo em conta as especificidades dos serviços em nuvem subcontratados nos seguintes domínios:

a. as atribuições e responsabilidades das funções da empresa envolvidas, em particular o OADS, e as funções responsáveis pelas TIC, pela segurança da informação, pela conformidade, pela gestão dos riscos e pela auditoria interna;

b. os processos e procedimentos de prestação de informação exigidos para a aprovação, execução, acompanhamento, gestão e renovação, se for caso disso, dos acordos de subcontratação de serviços de computação em nuvem relacionados com funções ou atividades operacionais essenciais ou importantes;

c. a supervisão dos serviços em nuvem proporcional à natureza, escala e complexidade dos riscos inerentes aos serviços prestados, incluindo i) a avaliação dos riscos associados aos acordos de subcontratação de serviços em nuvem e o dever de diligência («due diligence») relativamente aos prestadores de serviços de computação em nuvem, incluindo a frequência da avaliação do risco; ii) os controlos de acompanhamento e gestão (por exemplo, a verificação do acordo de nível de serviço); iii) as normas e controlos de segurança;

d. no que se refere à subcontratação de serviços em nuvem relacionados com funções ou atividades operacionais essenciais ou importantes, deve ser feita referência aos requisitos contratuais descritos na Orientação 10;

e. os requisitos de documentação e notificação escrita à autoridade de supervisão no que se refere à subcontratação de serviços em nuvem relacionados com funções ou atividades operacionais essenciais ou importantes;

f. no que diz respeito a cada acordo de subcontratação de serviços em nuvem que contemplem funções ou atividades operacionais essenciais ou importantes, a definição de uma «estratégia de saída» documentada e, quando adequado, suficientemente testada, proporcional à natureza, escala e complexidade dos riscos inerentes aos serviços prestados. A estratégia de saída pode envolver uma série de processos de rescisão, incluindo, entre outros, a interrupção, a reintegração ou a transferência dos serviços abrangidos pelo acordo de subcontratação.

Orientação 4 – Notificação por escrito à autoridade de supervisão

21. 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 autoridade de supervisão.

22. A notificação por escrito por parte da empresa deve incluir, tendo em conta o princípio da proporcionalidade, pelo menos as seguintes informações:

a. uma breve descrição da função ou atividade operacional subcontratada;

b. a data de início e, se for caso disso, a data da próxima renovação do contrato, a data do termo do contrato e/ou os períodos de pré-aviso aplicáveis ao prestador de serviços de computação em nuvem e à empresa;

c. a lei aplicável que rege o acordo de subcontratação de serviços em nuvem;

d. o nome do prestador de serviços de computação em nuvem, o número de registo da sociedade, o identificador da entidade jurídica (se existir), a sede

social e outras informações de contacto pertinentes, bem como o nome da empresa-mãe (se for caso disso); no caso de grupos, deve ser indicado se o prestador de serviços de computação em nuvem faz parte ou não do grupo;

e. o modelo do serviço de computação em nuvem e o modelo de implementação da nuvem (ou seja, nuvem pública/privada/híbrida/comunitária), bem como a natureza específica dos dados a conservar e os locais (ou seja, países ou regiões) onde esses dados serão armazenados;

f. um breve resumo das razões pelas quais a função ou atividade operacional subcontratada é considerada essencial ou importante;

g. a data da avaliação mais recente do caráter essencial ou da importância da função ou atividade operacional subcontratada.

Orientação 5 – Requisitos de documentação

23. No âmbito do seu sistema de governação e gestão de riscos, a empresa deve manter um registo de informações sobre o seus acordos de subcontratação de serviços de computação em nuvem, por exemplo, sob a forma de um registo dedicado e mantido atualizado ao longo do tempo. A empresa deve igualmente conservar, durante um período adequado e em conformidade com a legislação nacional, um registo dos acordos de subcontratação de serviços de computação em nuvem terminados.

24. Em caso de subcontratação de funções ou atividades operacionais essenciais ou importantes, a empresa deve registar todas as seguintes informações:

a. as informações a comunicar à autoridade de supervisão referidas na Orientação 4;

b. no caso de grupos, as empresas de seguros ou de resseguros e outras empresas abrangidas pela consolidação prudencial que recorram aos serviços de computação em nuvem;

c. a data da avaliação dos riscos mais recente e um breve resumo dos principais resultados;

d. o órgão individual ou decisório (por exemplo, o OADS) na empresa que aprovou o acordo de subcontratação de serviços de computação em nuvem;

e. as datas das auditorias mais recentes e das próximas auditorias agendadas, se aplicável;

f. os nomes dos subcontratantes aos quais sejam subcontratadas partes significativas de uma função ou atividade operacional essencial ou importante, incluindo o país em que os subcontratantes estão registados, o país em que será realizado o serviço e, se for caso disso, os locais (ou seja, países ou regiões) onde os dados serão armazenados;

g. o resultado da avaliação da substituibilidade do prestador de serviços de computação em nuvem (por exemplo, fácil, difícil ou impossível);

h. se a função ou atividade operacional essencial ou importante subcontratada apoia operações de negócio que sejam urgentes;

i. o custo anual orçamentado estimado;

j. se a empresa que procede à subcontratação possui uma estratégia de saída em caso de rescisão por uma das partes ou em caso de interrupção na prestação de serviços pelo prestador de serviços de computação em nuvem.

25. Em caso de subcontratação de funções ou atividades operacionais não essenciais ou não importantes, a empresa deve definir as informações a registar com base na natureza, escala e complexidade dos riscos inerentes aos serviços prestados pelo prestador de serviços de computação em nuvem.

26. A empresa deve disponibilizar à autoridade de supervisão, a pedido desta, todas as informações necessárias para permitir que esta efetue a supervisão da empresa, incluindo uma cópia do acordo de subcontratação.

Orientação 6 – Análise prévia à subcontratação

27. Antes de celebrar qualquer acordo com prestadores de serviços de computação em nuvem, a empresa deve:

a. avaliar se o acordo de subcontratação de serviços de computação em nuvem diz respeito a uma função ou atividade operacional essencial ou importante, em conformidade com a Orientação 7;

b. identificar e avaliar todos os riscos relevantes do acordo de subcontratação de serviços de computação em nuvem, em conformidade com a Orientação 8;

c. aplicar a diligência devida adequada ao potencial prestador de serviços de computação em nuvem, em conformidade com a Orientação 9;

d. identificar e avaliar os conflitos de interesses que a subcontratação possa implicar, em conformidade com os requisitos estabelecidos no artigo 274.º, n.º 3, alínea b), do Regulamento Delegado.

Orientação 7 – Avaliação das funções e atividades operacionais essenciais ou importantes («critical or important operational functions or activities»)

28. Antes de celebrar qualquer acordo de subcontratação a prestadores de serviços de computação em nuvem, a empresa deve avaliar se o acordo de subcontratação diz respeito a uma função ou atividade operacional que seja essencial ou importante. Ao proceder a essa avaliação, a empresa deve ter em conta, quando relevante, a possibilidade de as funções ou atividades operacionais contempladas pelo acordo virem a ser essenciais ou importantes no futuro. A empresa deve igualmente reavaliar o caráter essencial ou a importância da função ou atividade operacional anteriormente subcontratada a prestadores de serviços de computação em nuvem, se a natureza, a escala e a complexidade dos riscos inerentes ao acordo se alterarem substancialmente.

29. Na avaliação, a empresa deve ter em conta, em conjunto com o resultado da avaliação dos riscos, pelo menos, os seguintes fatores:

a. 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 sobre:

    i. o cumprimento contínuo das suas obrigações regulamentares;

    ii. a resiliência e a viabilidade financeira a curto e longo prazo;

    iii. a continuidade da atividade e a resiliência operacional;

    iv. o risco operacional, incluindo a conduta, as TIC e o risco legal;

    v. o risco reputacional;

b. o potencial impacto do acordo de subcontratação de serviços de computação em nuvem na capacidade da empresa para:

   i. identificar, monitorizar e gerir todos os riscos relevantes;

   ii. cumprir todos os requisitos legais e regulamentares;

   iii. realizar auditorias adequadas sobre a função ou atividade operacional subcontratada;

c. a exposição agregada da empresa (e/ou do grupo, se for caso disso) ao mesmo prestador de serviços em nuvem e o potencial impacto de acordos de subcontratação cumulativos na mesma área de atividade;

d. a dimensão e a complexidade de qualquer área de atividade afetada pelo acordo de subcontratação de serviços de computação em nuvem;

e. a capacidade para transferir o acordo de subcontratação proposto para outro prestador de serviços de computação em nuvem, se necessário ou desejável, ou reintegrar os serviços («substituibilidade»);

f. 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 dados, conforme previsto no Regulamento (UE) 2016/679[7], entre outras disposições regulamentares. A empresa deve ter especialmente em conta os dados sujeitos a sigilo comercial e/ou sensíveis (por exemplo, dados de saúde dos tomadores de seguros).

Orientação 8 – Avaliação dos riscos dos acordos de subcontratação de serviços de computação em nuvem

30. De um modo geral, a empresa deve adotar uma abordagem proporcional à natureza, escala e complexidade dos riscos inerentes aos serviços subcontratados a prestadores de serviços de computação em nuvem. Tal implica avaliar o potencial impacto dos acordos de subcontratação de serviços de computação em nuvem, em particular, nos seus riscos operacionais e reputacionais.

31. Quando subcontratarem funções ou atividades operacionais essenciais ou importantes a prestadores de serviços de computação em nuvem, as empresas devem:

a. ter em conta os benefícios e custos esperados do acordo proposto de subcontratação de serviços de computação em nuvem, incluindo a ponderação de quaisquer riscos significativos que possam ser reduzidos ou mais bem geridos face a quaisquer riscos significativos que possam resultar do acordo de subcontratação proposto;

b. avaliar, quando aplicável e adequado, os riscos, incluindo os riscos jurídicos, das TIC, de conformidade e de reputação, assim como as limitações de supervisão relacionadas com:

   i. o serviço de computação em nuvem selecionado e os modelos de implementação da nuvem propostos (ou seja, nuvem pública/privada/híbrida/comunitária);

   ii. a migração e/ou a implementação;

[7] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1).

iii. as atividades e os dados e sistemas associados que se pondere incluir no acordo de subcontratação (ou que já foram subcontratados), assim como a sua sensibilidade e as medidas de segurança necessárias;

iv. a situação de estabilidade política e de segurança dos países (pertencentes e não pertencentes à UE) em que os serviços subcontratados são ou podem ser prestados e em que os dados são, ou são suscetíveis de o serem, armazenados. A avaliação deve ter em conta:

1. as leis em vigor, incluindo as leis sobre proteção de dados;
2. as disposições de aplicação coerciva das leis em vigor;
3. as disposições legislativas em matéria de insolvência que seriam aplicáveis em caso de incumprimento de um prestador de serviços e eventuais restrições decorrentes da recuperação urgente dos dados da empresa;

v. a subcontratação em cadeia, incluindo os riscos adicionais que possam surgir se o subcontratante em cadeia estiver localizado num país terceiro ou num país diferente do prestador de serviços de computação em nuvem e o risco de que cadeias de subcontratação longas e complexas reduzam a capacidade da empresa para supervisionar as suas funções ou atividades operacionais essenciais ou importantes e a capacidade das autoridades de supervisão para as supervisionar de forma eficaz;

vi. o risco global de concentração quando várias empresas celebram acordos de subcontratação com um mesmo prestador de serviços de computação em nuvem, incluindo os casos em que é celebrado um acordo com um prestador de serviços que não é facilmente substituível ou em que são celebrados vários acordos de subcontratação com um único prestador de serviços em nuvem. Ao avaliar o risco de concentração, a empresa (e/ou o grupo, se for caso disso) deve ter em conta todos os seus acordos de subcontratação celebrados com esse prestador de serviços de computação em nuvem.

32. A avaliação de riscos deve ser efetuada antes de celebrar um acordo de subcontratação de serviços de computação em nuvem. Se a empresa tomar conhecimento de deficiências graves e/ou de alterações significativas nos serviços prestados ou na situação do prestador de serviços em nuvem, a avaliação de riscos deve ser imediatamente revista ou novamente realizada. Em caso de reformulação de um acordo de subcontratação de serviços de computação em nuvem para modificar o seu conteúdo e âmbito de aplicação (com vista, por exemplo, a alargar o âmbito de aplicação ou incluir funções operacionais essenciais ou importantes que não estavam anteriormente incluídas), deve ser efetuada uma reavaliação dos riscos.

Orientação 9 – Devida diligência («due diligence») em relação ao prestador de serviços de computação em nuvem

33. Durante o seu processo de seleção e avaliação, a empresa deve certificar-se de que o prestador de serviços de computação em nuvem é adequado à luz dos critérios definidos nos termos da sua política de subcontratação.

34. A devida diligência («due diligence») em relação ao prestador de serviços de computação em nuvem deve ser cumprida antes de subcontratar qualquer função ou atividade operacional. 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». Se a empresa tomar conhecimento de deficiências graves e/ou de alterações significativas nos serviços prestados ou na situação do prestador de serviços em nuvem, a situação deve ser imediatamente revista à luz dos procedimentos de devida diligência que, sendo necessário, devem ser novamente realizados.

35. Em caso de subcontratação de serviços de computação em nuvem relacionados com funções operacionais essenciais ou importantes, a diligência devida deverá incluir uma avaliação da adequação do prestador de serviços em nuvem (por exemplo, as suas competências, infraestruturas, situação financeira, estatuto empresarial e legal). Quando relevante, a empresa pode utilizar, como prova do cumprimento da sua devida diligência, certificações baseadas em normas internacionais, relatórios de auditoria de terceiros reconhecidos ou relatórios de auditoria interna.

Orientação 10 – Requisitos contratuais

36. Os direitos e obrigações da empresa e do prestador de serviços de computação em nuvem devem ser claramente identificados e especificados num acordo escrito.

37. Sem prejuízo dos requisitos enunciados no artigo 274.º do Regulamento Delegado, quando forem subcontratadas funções ou atividades operacionais essenciais ou importantes a um prestador de serviços de computação em nuvem, o acordo escrito de subcontratação deve estabelecer:

a. uma descrição clara da função subcontratada (serviços em nuvem, incluindo o tipo de serviço de apoio);

b. a data de início e a data de termo, se for caso disso, do acordo e os períodos de pré-aviso aplicáveis ao prestador de serviços de computação em nuvem e à empresa;

c. a jurisdição e a lei aplicável que regem o acordo;

d. as obrigações financeiras das partes;

e. se é permitida a subcontratação em cadeia de uma função ou atividade operacional essencial ou importante (ou partes significativas da mesma) e, em caso afirmativo, as condições a que está sujeita a subcontratação em cadeia (ver Orientação 13);

f. o(s) local(ais) (ou seja, regiões ou países) em que os dados relevantes serão armazenados e tratados (localização dos centros de dados) e as condições a cumprir, incluindo a obrigação de notificar a empresa caso o prestador de serviços pretenda alterar o(s) local(ais);

g. disposições relativas à acessibilidade, disponibilidade, integridade, confidencialidade, privacidade e segurança dos dados relevantes, tendo em conta as especificações enunciadas na Orientação 12;

h. o direito de a empresa acompanhar regularmente o desempenho do prestador de serviços de computação em nuvem;

i. os níveis de serviço acordados, que devem incluir objetivos de desempenho quantitativos e qualitativos concretos, a fim de permitir o acompanhamento em

tempo útil e a adoção sem demora de medidas corretivas adequadas, caso os níveis de serviço acordados não sejam cumpridos;

j. as obrigações de reporte do prestador de serviços de computação em nuvem à empresa, incluindo, se for caso disso, as obrigações de apresentação de relatórios relevantes para a função de segurança da empresa e para as suas principais funções, tais como relatórios da função de auditoria interna do prestador de serviços de computação em nuvem;

k. se o prestador de serviços de computação em nuvem deve subscrever um seguro obrigatório contra determinados riscos e, se for caso disso, o nível de cobertura exigido;

l. os requisitos de execução e ensaio dos planos de contingência;

m. a obrigação de o prestador de serviços de computação em nuvem conceder à empresa, às suas autoridades de supervisão e a qualquer outra pessoa designada pela empresa ou pelas autoridades de supervisão:

    i. pleno acesso a todas as instalações comerciais relevantes (sedes e centros de operações), incluindo todos os dispositivos, sistemas, redes, informações e dados relevantes utilizados no desempenho da função subcontratada, em especial, as informações financeiras conexas, o pessoal e os auditores externos do prestador de serviços de computação em nuvem («direitos de acesso e de informação»);

    ii. direitos ilimitados de inspeção e auditoria relacionados com o acordo de subcontratação de serviços de computação em nuvem («direitos de auditoria»), a fim de lhes permitir acompanhar o acordo de subcontratação e assegurar a conformidade com todos os requisitos regulamentares e contratuais aplicáveis;

n. disposições que assegurem que os dados detidos pela empresa possam ser imediatamente recuperados em caso de insolvência, resolução ou interrupção das operações de negócio do prestador de serviços em nuvem.

Orientação 11 – Direitos de acesso e de auditoria

38. O acordo de subcontratação de serviços de computação em nuvem não deverá limitar o exercício efetivo, por parte da empresa, dos direitos de acesso e de auditoria, bem como as opções de controlo sobre os serviços em nuvem, a fim de cumprir as suas obrigações regulamentares.

39. A empresa deve exercer os seus direitos de acesso e de auditoria, determinar a frequência das auditorias e os domínios e serviços a auditar, segundo uma abordagem baseada no risco, em conformidade com a seção 8 das Orientações da EIOPA sobre o sistema de governação.

40. Quando determinar a frequência e o âmbito dos seus direitos de acesso ou de auditoria, a empresa deve considerar se a subcontratação de serviços de computação em nuvem está relacionada com uma função ou atividade operacional essencial ou importante e ter em conta a natureza e dimensão do risco, assim como o impacto que os acordos de subcontratação de serviços de computação em nuvem representam para a empresa.

41. Se o exercício dos seus direitos de acesso ou de auditoria ou a utilização de determinados métodos de auditoria criarem riscos para o ambiente do prestador de serviços em nuvem e/ou de outro cliente (por exemplo, impacto nos níveis de serviço, disponibilidade de dados, questões de confidencialidade), a empresa e o prestador de serviços de computação em nuvem devem acordar formas alternativas

de fornecer à empresa um nível de garantia e de serviço semelhante (por exemplo, a inclusão de controlos específicos, a ser testado através de um relatório/certificação específico pelo prestador de serviços de computação em nuvem).

42. Sem prejuízo da sua responsabilidade final relativamente às atividades desempenhadas pelos seus prestadores de serviços de computação em nuvem e a fim de utilizar os recursos de auditoria com maior eficiência e reduzir os encargos administrativos para o prestador de serviços e os seus clientes, as empresas podem utilizar:

a. certificações de terceiros e relatórios de auditoria interna ou de terceiros disponibilizados pelo prestador de serviços de computação em nuvem;

b. auditorias comuns realizadas conjuntamente com outros clientes do mesmo fornecedor de serviços de computação em nuvem ou realizadas por terceiros por si designados.

43. No que respeita à subcontratação de funções ou atividades operacionais essenciais ou importantes, as empresas só devem utilizar o método referido na alínea a) do ponto 42 se:

a. assegurarem que o âmbito da certificação ou do relatório de auditoria abrange os sistemas (por exemplo, processos, aplicações, infraestruturas, centros de dados, etc.) e os controlos identificados pela empresa e permite avaliar o cumprimento dos requisitos regulamentares aplicáveis;

b. efetuarem uma avaliação exaustiva e regular do conteúdo das novas certificações ou dos relatórios de auditoria e verificarem se os relatórios ou as certificações não são obsoletos;

c. assegurarem que os sistemas e controlos fundamentais são incluídos em futuras versões da certificação ou do relatório de auditoria;

d. tiverem confirmado a aptidão da entidade de certificação ou de auditoria (por exemplo, no que se refere à rotatividade da empresa de certificação ou de auditoria, qualificações, conhecimentos especializados, repetição/verificação das provas no ficheiro de auditoria subjacente);

e. tiverem a certeza de que as certificações são emitidas e as auditorias são realizadas de acordo com as normas relevantes e incluem um teste da eficácia operacional dos controlos fundamentais existentes;

f. tiverem o direito contratual de solicitar a extensão do âmbito das certificações ou dos relatórios de auditoria a outros sistemas e controlos relevantes; o número e a frequência desses pedidos de alteração do âmbito devem ser razoáveis e legítimos do ponto de vista da gestão dos riscos;

g. mantiverem o direito contratual de realizar auditorias individuais no local, por sua livre iniciativa, no que diz respeito à subcontratação de serviços de computação em nuvem relacionados com funções ou atividades operacionais essenciais ou importantes; esse direito deve ser exercido em caso de necessidades específicas em que não seja possível interagir de outra forma com o prestador de serviços de computação em nuvem.

44. No que respeita à subcontratação de funções essenciais ou importantes a fornecedores de serviços de computação em nuvem, a empresa deve avaliar se as certificações e os relatórios de terceiros mencionados na alínea a) do ponto 42 são adequados e suficientes para cumprir as suas obrigações regulamentares e, numa abordagem baseada no risco, não devem ao longo do tempo recorrer exclusivamente a esses relatórios e certificações.

45. Antes de uma visita planeada ao local, a parte que exerce o seu direito de acesso (empresa, auditor ou terceiro atuando em nome das empresas) deve notificar a outra parte com uma antecedência razoável, a menos que tal não seja possível devido a uma situação de emergência ou de crise. Nessa notificação prévia, devem ser indicados a localização e o objetivo da visita, assim como o pessoal que participará na mesma.

46. Tendo em conta que as soluções de computação em nuvem têm um elevado nível de complexidade técnica, a empresa deve verificar se as pessoas que realizam a auditoria (sejam os seus auditores internos, o grupo de auditores que atua em seu nome, ou os auditores do prestador de serviços de computação em nuvem) ou, caso aplicável, as pessoas que fiscalizam a certificação de terceiros ou os relatórios de auditoria do prestador de serviços possuem as competências e os conhecimentos adequados para realizar as auditorias e/ou as avaliações relevantes.

Orientação 12 – Segurança dos dados e sistemas

47. A empresa deve garantir que os prestadores de serviços de computação em nuvem cumprem a legislação europeia e nacional, assim como as normas de segurança adequadas em matéria de TIC.

48. Quando forem subcontratadas funções ou atividades operacionais essenciais ou importantes a prestadores de serviços de computação em nuvem, a empresa deve ainda estabelecer no acordo de subcontratação requisitos específicos de segurança da informação e controlar regularmente o cumprimento desses requisitos.

49. Para efeitos do ponto 48, quando subcontratar funções ou atividades operacionais essenciais ou importantes a prestadores de serviços de computação em nuvem, a empresa, utilizando uma abordagem baseada no risco e tendo em conta as suas responsabilidades e as responsabilidades do prestador de serviços em nuvem, deverá:

a. definir e distinguir de forma clara as competências e responsabilidades que cabem ao prestador de serviços e à empresa relativamente às funções ou atividades operacionais abrangidas pelo acordo de subcontratação;

b. definir e decidir um nível adequado de proteção de dados confidenciais, de continuidade das atividades subcontratadas e da integridade e rastreabilidade dos dados e sistemas no contexto da subcontratação de serviços de computação em nuvem pretendida;

c. considerar medidas específicas, se necessário, no que respeita a dados em trânsito, dados em memória e dados armazenados, como a utilização de tecnologias de encriptação, em conjugação com uma arquitetura de gestão de chaves adequada;

d. considerar os mecanismos de integração dos serviços em nuvem com os sistemas das empresas, por exemplo, as interfaces de programação de aplicações e um processo eficiente de gestão de acesso e de utilizador;

e. assegurar contratualmente que a disponibilidade e a capacidade de tráfego da rede prevista cumprem requisitos de continuidade rigorosos, quando aplicável e exequível;

f. definir e estabelecer requisitos de continuidade apropriados que garantam níveis de desempenho adequados em cada nível da cadeia tecnológica, quando aplicável;

g. utilizar um processo de gestão de incidentes consistente e bem documentado, incluindo as respetivas responsabilidades, por exemplo, através da definição de um modelo de cooperação em caso de ocorrência ou de suspeitas de incidentes;

h. adotar uma abordagem baseada no risco para o(s) local(is) de armazenamento e de tratamento de dados (ou seja, país ou região), bem como considerações em matéria de segurança da informação;

i. controlar o cumprimento dos requisitos relativos à eficácia e eficiência dos mecanismos de controlo implementados pelo prestador de serviços de computação em nuvem que permitem atenuar os riscos inerentes aos serviços prestados.

Orientação 13 – Subcontratação em cadeia de funções ou atividades operacionais essenciais ou importantes

50. Se a subcontratação em cadeia de funções operacionais essenciais ou importantes (ou de parte das mesmas) for autorizada, o acordo de subcontratação de serviços de computação em nuvem deve:

a. especificar os tipos de atividades que são excluídas da possível subcontratação em cadeia;

b. indicar as condições a respeitar em caso de subcontratação em cadeia (por exemplo, igual cumprimento integral, por parte do subcontratante em cadeia, das obrigações impostas ao prestador de serviços de computação em nuvem). Estas obrigações incluem os direitos de acesso e de auditoria, assim como a garantia de segurança dos dados e sistemas;

c. indicar que o prestador de serviços de computação em nuvem é obrigado a supervisionar os serviços que subcontratou em cadeia e assume a plena responsabilidade pelos mesmos;

d. incluir a obrigação de o prestador de serviços de computação em nuvem informar a empresa de qualquer alteração prevista nos subcontratantes em cadeia ou nos serviços subcontratados em cadeia, suscetível de afetar a capacidade do prestador de serviços de cumprir com as suas responsabilidades no âmbito do acordo de subcontratação de serviços de computação em nuvem. O prazo de notificação dessas alterações deve permitir que a empresa realize, pelo menos, uma avaliação dos riscos que as alterações propostas representam antes de estas serem implementadas;

e. quando um prestador de serviços de computação em nuvem planear introduzir alterações num subcontratante em cadeia ou em serviços subcontratados em cadeia, suscetíveis de afetar negativamente a avaliação de riscos dos serviços acordados, assegurar que a empresa tem o direito de se opor a tais alterações e/ou de rescindir e abandonar o contrato.

Orientação 14 – Acompanhamento e supervisão de acordos de subcontratação de serviços de computação em nuvem

51. A empresa deve acompanhar permanentemente as atividades dos seus prestadores de serviços de computação em nuvem, assim como as medidas de segurança e o cumprimento do nível de serviço acordado, segundo uma abordagem baseada no risco, prestando especial atenção à subcontratação de funções operacionais essenciais e importantes.

52. Para esse efeito, a empresa deverá criar mecanismos de acompanhamento e supervisão, que deverão ter em conta, sempre que possível e adequado, a existência de subcontratação em cadeia de funções operacionais essenciais ou importantes ou de uma parte das mesmas.

53. O OADS deve ser regularmente informado sobre os riscos identificados na subcontratação de funções ou atividades operacionais essenciais ou importantes.

54. A fim de assegurar o acompanhamento e a supervisão adequados dos seus acordos de subcontratação de serviços de computação em nuvem, as empresas devem mobilizar recursos suficientes com competências e conhecimentos adequados para monitorizar os serviços em nuvem subcontratados. O pessoal da empresa responsável por estas atividades deve possuir os meios informáticos e tecnológicos necessários, assim como os devidos conhecimentos sobre a área de atividade.

Orientação 15 – Direitos de rescisão e estratégias de saída

55. Quando forem subcontratados serviços de computação em nuvem relacionados com funções ou atividades operacionais essenciais ou importantes, a empresa deve dispor, ao abrigo do acordo de subcontratação em causa, de uma estratégia de saída claramente definida, que garanta a possibilidade de pôr termo ao acordo, se necessário. Deverá ser possível rescindir o acordo sem prejudicar a continuidade e a qualidade dos serviços prestados aos tomadores de seguros. Para esse efeito, a empresa deve:

a. elaborar e implementar planos de saída abrangentes, baseados em serviços, documentados e suficientemente testados (por exemplo, realizando uma análise dos potenciais custos, impactos, recursos e implicações em termos de calendarização das várias opções de saída viáveis);

b. identificar soluções alternativas e elaborar planos de transição adequados e viáveis que permitam à empresa eliminar as atividades e dados subcontratados ao prestador de serviços em nuvem e transferi-los para prestadores de serviços alternativos ou para a própria empresa. Estas soluções devem ser definidas tendo em conta os desafios que possam surgir devido à localização dos dados e adotando as medidas necessárias para garantir a continuidade da atividade durante a fase de transição;

c. assegurar que o prestador de serviços de computação em nuvem apoie adequadamente a empresa durante o processo de transferência de dados, sistemas ou aplicações subcontratados para outro prestador de serviços ou para a própria empresa;

d. acordar com o prestador de serviços de computação em nuvem que, depois de retransferidos para a empresa, os dados da empresa serão integralmente apagados de forma segura pelo prestador de serviços em todas as regiões.

56. Quando elaborar estratégias de saída, a empresa deve:

a. definir os objetivos da estratégia de saída;

b. definir os fatores (por exemplo, indicadores-chave de risco alertando para um nível de serviço inaceitável) que deverão desencadear a saída;

c. realizar uma análise do impacto das atividades que seja proporcional às atividades subcontratadas, a fim de identificar os recursos humanos e materiais que seriam necessários para implementar o plano de saída e o tempo necessário para executá-lo;

d. atribuir funções e responsabilidades para gerir os planos de saída e o processo de transição;

e. definir critérios de sucesso para a transição.

Orientação 16 – Supervisão dos acordos de subcontratação de serviços de computação em nuvem pelas autoridades competentes

57. As autoridades de supervisão devem analisar os impactos decorrentes dos acordos de subcontratação de serviços de computação em nuvem celebrados pelas empresas, no âmbito dos seus processos de avaliação em sede de supervisão. A análise dos impactos deve incidir, em particular, nas disposições relacionadas com a subcontratação de funções ou atividades operacionais essenciais ou importantes.

58. Ao supervisionar os acordos de subcontratação de serviços de computação em nuvem celebrados pelas empresas, as autoridades de supervisão devem ter em conta os seguintes riscos:

a. os riscos relacionados com as TIC;

b. outros riscos operacionais (incluindo os riscos jurídicos e de conformidade, os riscos associados à subcontratação e gestão por terceiros);

c. os riscos reputacionais;

d. os riscos de concentração, incluindo a nível nacional/setorial.

59. Na sua avaliação, as autoridades de supervisão devem incluir os seguintes aspetos numa abordagem baseada no risco:

a. a adequação e eficácia dos processos operacionais e de governação da empresa relacionados com a aprovação, execução, acompanhamento, gestão e renovação dos acordos de subcontratação de serviços de computação em nuvem;

b. se a empresa dispõe de recursos suficientes, com competências e conhecimentos adequados, para acompanhar os serviços de computação em nuvem subcontratados;

c. se a empresa identifica e gere todos os riscos referidos nas presentes orientações.

60. No caso de grupos, o supervisor do grupo deve assegurar que os impactos da subcontratação de serviços de computação em nuvem relacionados com funções ou atividades operacionais essenciais ou importantes sejam refletidos na avaliação do risco de supervisão do grupo, tendo em conta os requisitos enumerados nos pontos 58 e59, assim como a governação e as características operacionais individuais do grupo.

61. Se o acordo de subcontratação de serviços de computação em nuvem relacionados com funções ou atividades operacionais essenciais ou importantes envolver mais do que uma empresa em diferentes Estados-Membros e for gerido centralmente pela empresa-mãe ou por uma filial do grupo (por exemplo, uma empresa de serviços por conta da empresa ou do grupo, como o prestador de serviços TIC do grupo), o supervisor do grupo e/ou as autoridades competentes para supervisionar as empresas envolvidas na subcontratação de serviços de computação em nuvem devem discutir, no seio do colégio de supervisores, quando relevante, os impactos que o acordo de subcontratação poderá ter no perfil de risco do grupo.

62. Sempre que sejam identificadas preocupações que permitam concluir que uma empresa já não dispõe de mecanismos de governação sólidos ou não cumpre os requisitos regulamentares, as autoridades competentes devem adotar medidas adequadas, que podem incluir, por exemplo, a exigência à empresa no sentido de melhorar o seu mecanismo de governação, a limitação ou a restrição do âmbito das

funções subcontratadas ou a exigência da saída de um ou mais acordos de subcontratação. Em especial, tendo em conta a necessidade de assegurar a continuidade da atividade da empresa, a cessação de contratos poderá ser necessária caso não seja possível assegurar a supervisão e aplicação dos requisitos regulamentares através de outras medidas.

Regras relativas ao cumprimento e à comunicação de informações

63. O presente documento contém orientações emitidas ao abrigo do artigo 16.º do Regulamento (UE) n.º 1094/2010. Nos termos do artigo 16.º, n.º 3, desse regulamento, as autoridades competentes e as instituições financeiras devem desenvolver todos os esforços para dar cumprimento às orientações e recomendações.

64. As autoridades competentes que cumpram ou tencionem dar cumprimento às presentes Orientações devem incorporá-las de forma adequada no seu quadro regulamentar ou de supervisão.

65. As autoridades competentes devem confirmar perante a EIOPA se cumprem ou tencionam dar cumprimento às presentes Orientações, indicando as razões para o não cumprimento, no prazo de dois meses a contar da data de publicação das versões traduzidas.

66. Na falta de uma resposta no prazo referido, as autoridades competentes serão consideradas incumpridoras da obrigação de comunicação e declaradas como tal.

Disposição final relativa à revisão

67. As presentes orientações devem ser objeto de revisão pela EIOPA.