EBA/GL/2019/02

25 de fevereiro de 2019

Orientações relativas à subcontratação

1. Obrigações de cumprimento e de comunicação de informação

Natureza das presentes orientações

1. O presente documento contém orientações emitidas ao abrigo do artigo 16.º do Regulamento (UE) n.º 1093/2010[1]. Nos termos do artigo 16.º, n.º 3, do Regulamento (UE) n.º 1093/2010, as autoridades competentes e as instituições financeiras devem desenvolver todos os esforços para dar cumprimento às orientações.

2. As orientações definem a posição da EBA sobre o que constituem práticas de supervisão adequadas no âmbito do Sistema Europeu de Supervisão Financeira ou sobre o modo como a legislação da União deve ser aplicada num domínio específico. As autoridades competentes, na aceção do artigo 4.º, n.º 2, do Regulamento (UE) n.º 1093/2010, às quais as orientações se aplicam, devem dar cumprimento às mesmas, incorporando-as nas suas práticas conforme for mais adequado (por exemplo, alterando o seu enquadramento jurídico ou os seus processos de supervisão), incluindo nos casos em que as orientações são dirigidas em primeiro lugar a instituições e instituições de pagamento.

Requisitos de comunicação de informação

3. Nos termos do disposto no artigo 16.º, n.º 3, do Regulamento (UE) n.º 1093/2010, as autoridades competentes confirmam à EBA se dão ou tencionam dar cumprimento às presentes Orientações ou, caso contrário, indicam as razões para o não cumprimento até ([dd.mm.aaaa]). Na ausência de qualquer notificação até à referida data, a EBA considera que as autoridades competentes em causa não cumprem as orientações. As notificações efetuam-se mediante o envio do formulário disponível no sítio Web da EBA para o endereço compliance@eba.europa.eu com a referência «EBA/GL/2019/02». As notificações devem ser efetuadas por pessoas devidamente autorizadas a notificar a situação de cumprimento em nome das respetivas autoridades competentes. Qualquer alteração no que respeita à situação de cumprimento deve igualmente ser comunicada à EBA.

4. As notificações serão publicadas no sítio Web da EBA, em conformidade com o artigo 16.º, n.º 3.

[1] Regulamento (UE) n.º 1093/2010 do Parlamento Europeu e do Conselho, de 24 de novembro de 2010, que cria uma Autoridade Europeia de Supervisão (Autoridade Bancária Europeia), altera a Decisão n.º 716/2009/CE e revoga a Decisão 2009/78/CE da Comissão (JO L 331 de 15.12.2010, p. 12).

2. Objeto, âmbito de aplicação e definições

Objeto

5. As presentes orientações especificam as disposições de governo interno, incluindo uma gestão de riscos sã, que as instituições, as instituições de pagamento e as instituições de moeda eletrónica devem implementar quando subcontratam funções, em particular no que se refere à subcontratação de funções essenciais e importantes.

6. As orientações especificam o modo como as disposições mencionadas no parágrafo anterior devem ser revistas e avaliadas pelas autoridades competentes no contexto do artigo 97.º da Diretiva 2013/36/UE[2], do processo de análise e avaliação pelo supervisor (SREP), do artigo 9.º, n.º 3, da Diretiva (UE) 2015/2366[3] e do artigo 5.º, n.º 5 da Diretiva 2009/110/CE[4], no exercício do seu dever de monitorizar a conformidade contínua das entidades destinatárias das presentes orientações com as condições das respetivas autorizações.

Destinatários

7. As presentes orientações destinam-se às autoridades competentes na aceção do artigo 4. º, n.º 1, ponto 40, do Regulamento (UE) n.º 575/2013[5], incluindo o Banco Central Europeu no âmbito das matérias relacionadas com as funções que lhe foram conferidas pelo Regulamento (UE) n.º 1024/2013[6], às instituições de crédito definidas no artigo 4. º, n.º 1, ponto 3, do Regulamento (UE) n.º 575/2013, às instituições de pagamento definidas no artigo 4. º, n.º 4, da Diretiva (UE) n.º 2015/2366 e às instituições de moeda eletrónica definidas no artigo 2. º, n.º 1, da Diretiva 2009/110/CE. Os prestadores de serviços de informação sobre contas que apenas prestam serviço ao abrigo do ponto 8 do Anexo I da Diretiva (UE) 2015/2366 não são incluídos no âmbito de aplicação das presentes orientações, em conformidade com o artigo 33.º da referida diretiva.

---

[2]Diretiva 2013/36/UE do Parlamento Europeu e do Conselho, de 26 de junho de 2013, relativa ao acesso à atividade das instituições de crédito e à supervisão prudencial das instituições de crédito e empresas de investimento, que altera a Diretiva 2002/87/CE e revoga as Diretivas 2006/48/CE e 2006/49/CE

[3]Diretiva 2015/2366/UE do Parlamento Europeu e do Conselho, de 25 de novembro de 2015, relativa aos serviços de pagamento no mercado interno, que altera as Diretivas 2002/65/CE, 2009/110/CE, 2013/36/UE e o Regulamento (UE) n.º 1093/2010 e revoga a Diretiva 2007/64/CE.

[4]Diretiva 2009/110/CE do Parlamento Europeu e do Conselho, de 16 de setembro de 2009, relativa ao acesso à atividade das instituições de moeda eletrónica, ao seu exercício e à sua supervisão prudencial, que altera as Diretivas 2005/60/CE e 2006/48/CE e revoga a Diretiva 2000/46/CE.

[5] Regulamento (UE) n.º 575/2013 do Parlamento Europeu e do Conselho, de 26 de junho de 2013, relativo aos requisitos prudenciais para as instituições de crédito e empresas de investimento e que altera o Regulamento (UE) n.º 648/2012 (JO L 176 de 27.6.2013, p. 1).

[6] Regulamento (UE) 1024/2013 do Conselho, de 15 de outubro de 2013, que confere ao Banco Central Europeu atribuições específicas no que diz respeito às políticas relativas à supervisão prudencial das instituições de crédito.

8. Para efeitos das presentes orientações, qualquer referência a «instituições de pagamento» inclui «instituições de moeda eletrónica» e qualquer referência a «serviços de pagamento» inclui «emissão de moeda eletrónica».

Âmbito de aplicação

9. Sem prejuízo da Diretiva 2014/65/UE [7] e do Regulamento Delegado (UE) 2017/565 [8] da Comissão (que contém requisitos relativos à subcontratação por instituições que prestam serviços e realizam atividades de investimento, bem como orientações relevantes emitidas pela Autoridade Europeia dos Valores Mobiliários e dos Mercados relativamente a serviços e atividades de investimento), as instituições definidas no artigo 3.º, n.º 1, ponto 3, da Diretiva 2013/36/UE devem cumprir as presentes orientações em base individual, em base subconsolidada e em base consolidada. A aplicação em base individual pode ser objeto de isenção pelas autoridades competentes ao abrigo do artigo 21.º da Diretiva 2013/36 ou do artigo 109.º, n.º 1 da Diretiva 2013/36/UE em conjunção com o artigo 7.º do Regulamento (UE) n.º 575/2013. As instituições sujeitas à Diretiva 2013/36/UE devem cumprir a mesma e as presentes orientações numa base consolidada e subconsolidada, tal como estabelecido no artigo 21.º e nos artigos 108.º a 110.º da Diretiva 2013/36/UE.

10. Sem prejuízo do artigo 8.º, n.º 3, da Diretiva (UE) 2015/2366 e do artigo 5.º, n.º 7, da Diretiva 2009/110/CE, as instituições de pagamento e as instituições de moeda eletrónica devem cumprir as presentes orientações em base individual.

11. As autoridades competentes responsáveis pela supervisão das instituições, das instituições de pagamento e das instituições de moeda eletrónica devem cumprir as presentes orientações.

Definições

12. Salvo indicação em contrário, os termos utilizados e definidos na Diretiva 2013/36/UE, no Regulamento (UE) n.º 575/2013, na Diretiva 2009/110/CE, na Diretiva (UE) 2015/2366 e nas Orientações da EBA sobre governo interno [9] têm o mesmo significado nas presentes orientações. Adicionalmente, para efeitos das presentes orientações, aplicam-se as seguintes definições:

Subcontratação	Um acordo, independentemente da sua forma, celebrado entre uma instituição, uma instituição de pagamento ou uma instituição de moeda

[7] Diretiva 2014/65/UE do Parlamento Europeu e do Conselho, 15 de maio de 2014, relativa aos mercados de instrumentos financeiros e que altera a Diretiva 2002/92/CE e a Diretiva 2011/61/UE (JO L 173, de 12.6.2014, p. 349).

[8] Regulamento Delegado (UE) 2017/565 da Comissão, de 25 de abril de 2016, que completa a Diretiva 2014/65/UE do Parlamento Europeu e do Conselho no que diz respeito aos requisitos em matéria de organização e às condições de exercício da atividade das empresas de investimento e aos conceitos definidos para efeitos da referida diretiva (JO L 87, de 31.3.2017, p. 1).

[9] https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised-

	eletrónica e um prestador de serviços, nos termos do qual esse prestador de serviços realiza um processo, presta um serviço ou desenvolve uma atividade que, de outro modo, seriam realizados pela própria instituição, pela própria instituição de pagamento ou pela própria instituição de moeda eletrónica.
Função	Quaisquer processos, serviços ou atividades.
Funções essenciais ou importantes[10]	Quaisquer funções que sejam consideradas essenciais ou importantes na aceção da Secção 4 das presentes orientações.
Sub-subcontratação	Situação em que o prestador de serviços, ao abrigo de um acordo de subcontratação, transfere uma função subcontratada para outro prestador de serviços.[11]
Prestador de serviços	Entidade terceira que realiza, no todo ou em parte, uma atividade, um processo ou um serviço subcontratado, 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	Infraestrutura em nuvem disponível para utilização exclusiva por uma única instituição ou instituição de pagamento.
Nuvem comunitária	Infraestrutura em nuvem disponível para utilização exclusiva por uma comunidade específica de instituições ou instituições de pagamento, incluindo várias instituições de um único grupo.
Nuvem híbrida	Infraestrutura em nuvem composta por duas ou mais infraestruturas em nuvem distintas.

[10] A expressão «função essencial ou importante» baseia-se na formulação utilizada na Diretiva 2014/65/UE (MiFID II) e no Regulamento Delegado (UE) 2017/565 da Comissão que complementa a MiFID II e é utilizada apenas para efeitos de subcontratação; não está relacionada com a definição de «funções críticas» para efeitos do quadro de recuperação e resolução, conforme definido no artigo 2.º, n.º 1, ponto 35, da Diretiva 2014/59/UE (DRRB).

[11] Para a avaliação, aplicam-se as disposições da Secção 3; a sub-subcontratação é também designada, em outros documentos EBA, por «cadeia de subcontratação» ou por «subcontratação em cadeia».

Órgão de administração	Órgão ou órgãos de uma instituição ou instituição de pagamento, nomeados em conformidade com a legislação nacional, com poderes para definir a estratégia, os objetivos e a orientação geral da instituição ou da instituição de pagamento, que supervisionam e monitorizam o processo de tomada de decisões de gestão e que integram as pessoas que dirigem efetivamente as atividades da instituição ou da instituição de pagamento, bem como os diretores e pessoas responsáveis pela gestão da instituição de pagamento.

3. Implementação

Data de aplicação

13. À exceção do parágrafo 63 alínea b), as presentes orientações são aplicáveis a partir de 30 de setembro de 2019 a todos os acordos de subcontratação celebrados, revistos ou alterados a partir dessa data. O parágrafo 63 alínea b) é aplicável a partir de 31 de dezembro de 2021.

14. As instituições e instituições de pagamento devem rever e alterar adequadamente os acordos de subcontratação existentes, de modo a garantir a conformidade dos mesmos com as presentes orientações.

15. Se a revisão dos acordos de subcontratação de funções essenciais ou importantes não estiver concluída até 31 de dezembro de 2021, as instituições e instituições de pagamento devem informar a suas autoridades competentes dessa circunstância, incluindo as medidas previstas para concluir a revisão ou a eventual estratégia de saída de tais acordos.

Disposições transitórias

16. As instituições e instituições de pagamento devem completar a documentação de todos os acordos de subcontratação existentes, exceto os acordos de subcontratação com fornecedores de serviços em nuvem, de acordo com as presentes orientações após a primeira data de renovação de cada contrato de subcontratação vigente, mas o mais tardar até 31 de dezembro de 2021.

Revogação

17. As orientações do Comité das Autoridades Europeias de Supervisão Bancária (CAESB) de 14 de dezembro de 2006 sobre a subcontratação e as recomendações da EBA relativas à subcontratação externa a prestadores de serviços de computação em nuvem [12]são revogadas com efeitos a partir de 30 de setembro de 2019.

[12] Recomendações relativas à subcontratação externa a prestadores de serviços de computação em nuvem (EBA/REC/2017/03).[12]

4. Orientações relativas à subcontratação

Título I – Proporcionalidade: apresentação de pedidos em grupo e sistemas de proteção institucional

1 Proporcionalidade

18. As instituições, as instituições de pagamento e as autoridades competentes, ao darem cumprimento às presentes orientações ou ao supervisionarem o seu cumprimento, devem ter em conta o princípio da proporcionalidade. Este princípio visa assegurar que os sistemas de governo, nomeadamente os relacionados com a subcontratação, sejam consistentes com o perfil de risco individual, a natureza e o modelo de negócio da instituição ou da instituição de pagamento, bem como com o nível e a complexidade das suas atividades, de modo a que os objetivos dos requisitos regulamentares sejam efetivamente alcançados.

19. Quando aplicam os requisitos estabelecidos nas presentes orientações, as instituições e as instituições de pagamento devem ter em conta a complexidade das funções subcontratadas, os riscos decorrentes do acordo de subcontratação, o caráter essencial ou a importância da função subcontratada e o potencial impacto da subcontratação na continuidade das suas atividades.

20. Quando aplicam o princípio da proporcionalidade, as instituições, as instituições de pagamento[13] e as autoridades competentes devem ter em conta os critérios especificados no Título I das Orientações da EBA sobre governo interno, em conformidade com o artigo 74.º, n.º 2, da Diretiva 2013/36/UE.

2 Subcontratação em grupos e instituições que sejam membros de um sistema de proteção institucional

21. Nos termos do artigo 109.º, n.º 2, da Diretiva 2013/36/UE, as presentes orientações devem também ser aplicáveis em base subconsolidada ou consolidada, tendo em conta o âmbito

[13] As instituições de pagamento devem igualmente consultar as orientações da EBA relativas às informações a prestar para a autorização de instituições de pagamento e de instituições de moeda eletrónica e para o registo dos prestadores de serviços de informação sobre contas, ao abrigo da Diretiva Serviços de Pagamento revista (DSP2), disponíveis no sítio Web da EBA no seguinte endereço: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2

prudencial da consolidação[14]. Para o efeito, as empresas-mãe da UE ou a empresa-mãe num Estado-Membro devem assegurar que os sistemas, processos e mecanismos de governo interno nas suas filiais, incluindo as instituições de pagamento, sejam consistentes, bem integrados e adequados para a aplicação efetiva das presentes orientações a todos os níveis relevantes.

22. As instituições e as instituições de pagamento, nos termos do ponto 21, e as instituições que, enquanto membros de um sistema de proteção institucional, utilizem sistemas de governo disponibilizados a nível central, devem cumprir os seguintes requisitos:

    a. sempre que essas instituições ou instituições de pagamento tenham celebrado acordos de subcontratação com prestadores de serviços dentro do grupo ou do sistema de proteção institucional[15], o órgão de administração dessas instituições ou instituições de pagamento é também, no que respeita a esses acordos de subcontratação, plenamente responsável pelo cumprimento de todos os requisitos regulamentares e pela aplicação efetiva das presentes orientações;

    b. sempre que essas instituições ou instituições de pagamento subcontratem as tarefas operacionais das funções de controlo interno a um prestador de serviços dentro do grupo ou do sistema de proteção institucional, para fins de acompanhamento e auditoria dos acordos de subcontratação, as instituições devem garantir que, também no que respeita a esses acordos de subcontratação, essas tarefas operacionais sejam efetivamente executadas, nomeadamente através da receção de relatórios adequados.

23. Além do disposto no ponto 22, as instituições e as instituições de pagamento de um grupo ao qual não tenham sido concedidas isenções com base no artigo 109.º da Diretiva 2013/36/UE e no artigo 7.º do Regulamento (UE) n.º 575/2013, as instituições que sejam um organismo central ou que estejam filiadas de modo permanente a um organismo central ao qual não tenham sido concedidas isenções com base no artigo 21.º da Diretiva 2013/36/UE, ou as instituições que sejam membros de um sistema de proteção institucional, devem ter em conta o seguinte:

    a. sempre que o acompanhamento operacional da subcontratação seja centralizado (p. ex., no âmbito de um acordo-quadro destinado ao acompanhamento de acordos de subcontratação), as instituições e as instituições de pagamento devem garantir que seja possível realizar, pelo menos no que respeita às funções essenciais ou importantes subcontratadas, tanto o acompanhamento independente do prestador de serviços como a supervisão adequada por cada instituição ou instituição de pagamento, nomeadamente através da receção, pelo menos, uma vez por ano e mediante pedido da função de acompanhamento centralizado, de relatórios que incluam, no mínimo,

[14] Consultar o artigo 4.º, n.º 1, pontos 47 e 48, do Regulamento (UE) n.º 575/2013, no que respeita ao âmbito da consolidação.

[15] Nos termos do artigo 113.º, n.º 7, do RRFP, entende-se por sistema de proteção institucional um acordo de responsabilidade contratual ou legal que protege as instituições que sejam membros desse sistema e, em particular, garante a respetiva liquidez e solvência a fim de evitar a falência, se necessário.

um resumo da avaliação dos riscos e do acompanhamento do desempenho. Além disso, as instituições e as instituições de pagamento devem receber da função de acompanhamento centralizado um resumo dos relatórios de auditoria relevantes de subcontratação de funções essenciais ou importantes e, mediante pedido, o relatório de auditoria completo;

b. as instituições e as instituições de pagamento devem garantir que o seu órgão de administração seja devidamente informado das alterações importantes previstas no que respeita aos prestadores de serviços que sejam objeto de acompanhamento centralizado, bem como do potencial impacto dessas alterações nas funções essenciais ou importantes prestadas, nomeadamente um resumo da análise dos riscos que inclua o risco legal, o cumprimento dos requisitos regulamentares e o impacto nos níveis de serviço, para que possam avaliar o impacto dessas alterações;

c. sempre que essas instituições e instituições de pagamento num grupo, instituições que estejam filiadas num organismo central ou instituições que façam parte de um sistema de proteção institucional se baseiem numa avaliação central prévia dos acordos de subcontratação, conforme referido na secção 12, cada instituição e instituição de pagamento deve receber um resumo dessas avaliações e garantir que estas têm em consideração a sua estrutura específica e os seus riscos específicos no âmbito do processo de tomada decisão;

d. sempre que o registo de todos os acordos de subcontratação existentes, conforme referido na secção 11, seja criado e mantido centralmente no âmbito de um grupo ou de um sistema de proteção institucional, as autoridades competentes e todas as instituições e instituições de pagamento devem ser capazes de obter o seu registo individual sem demora indevida. Este registo deve incluir todos os acordos de subcontratação, incluindo os acordos celebrados com prestadores de serviços que sejam membros desse grupo ou desse sistema de proteção institucional;

e. sempre que essas instituições e instituições de pagamento recorram a um plano de saída para uma função essencial ou importante que tenha sido estabelecido a nível do grupo, no âmbito no sistema de proteção institucional ou pelo organismo central, todas as instituições e instituições de pagamento devem receber um resumo do plano e certificarem-se de que o plano pode ser efetivamente executado.

24. Sempre que tenham sido concedidas isenções nos termos do artigo 21.º da Diretiva 2013/36/UE ou do artigo 109.º, n.º 1, da mesma diretiva em conjunto com o artigo 7.º do Regulamento (UE) n.º 575/2013, as disposições das presentes orientações devem ser aplicadas pela empresa-mãe num Estado-Membro, a si própria e às suas filiais, ou pelo organismo central e pelas suas filiais no seu todo.

25. As instituições e as instituições de pagamento que sejam filiais de uma empresa-mãe da UE ou de uma empresa-mãe num Estado-Membro à qual não tenham sido concedidas isenções com

base no artigo 21.º da Diretiva 2013/36/UE ou do artigo 109.º, n.º 1, da mesma diretiva, em conjunto com o artigo 7.º do Regulamento (UE) n.º 575/2013, devem assegurar que cumprem individualmente as presentes orientações em base individual.

Título II – Avaliação dos acordos de subcontratação

3 Subcontratação

26. As instituições e as instituições de pagamento devem determinar se um acordo celebrado com uma entidade terceira é abrangido pela definição de subcontratação. No âmbito desta avaliação, deve ser tido em consideração se a função (ou parte da mesma) que é objeto de subcontratação a um prestador de serviços é executada de uma forma periódica ou contínua pelo prestador de serviços e se essa função (ou parte da mesma) seria normalmente abrangida pelo âmbito das funções que seriam ou poderiam realisticamente ser desempenhadas pelas instituições ou pelas instituições de pagamento, mesmo que a instituição ou a instituição de pagamento não tenha desempenhado anteriormente essa função.

27. Sempre que um acordo celebrado com um prestador de serviços abranja várias funções, as instituições e as instituições de pagamento devem ter em conta todos os aspetos do acordo no âmbito da sua avaliação – por exemplo, se o serviço prestado incluir o fornecimento de dispositivos de armazenamento e a cópia de segurança dos dados, ambos aspetos devem ser considerados em conjunto.

28. Como princípio geral, as instituições e as instituições de pagamento não devem considerar como subcontratação:

    a. uma função que, legalmente, deva ser desempenhada por um prestador de serviços, p. ex, a revisão legal de contas;

    b. serviços de informação sobre mercados (p. ex., fornecimento de dados pela Bloomberg, Moody's, Standard & Poor's, Fitch);

    c. infraestruturas de rede globais (p. ex., Visa, MasterCard);

    d. sistemas de compensação e de liquidação entre câmaras de compensação, contrapartes centrais e instituições de liquidação e respetivos membros;

    e. infraestruturas globais de mensagens financeiras sujeitas a supervisão das autoridades competentes;

    f. serviços de correspondente bancário; e

    g. a aquisição de serviços que, de outro modo, não seriam realizados pela instituição ou pela instituição de pagamento (p. ex., aconselhamento de um arquiteto, emissão de parecer jurídico e representação perante órgãos judiciais e administrativos, serviços de

limpeza, jardinagem e manutenção das instalações da instituição ou da instituição de pagamento, serviços médicos, serviço pós-venda de viaturas de empresa, restauração, serviços de máquinas de venda automática, serviços de escritório, serviços de viagens, serviços postais, rececionistas, secretários e telefonistas), bens (p. ex., cartões de plástico, leitores de cartões, material de escritório, computadores pessoais, mobiliário) ou serviços de utilidade pública (p. ex., eletricidade, gás, água, linha telefónica).

4 Funções essenciais ou importantes

29. As instituições e as instituições de pagamento devem sempre considerar uma função como essencial ou importante nas seguintes situações[16]:

    a. se uma falha ou o insucesso no seu desempenho materialmente implicar:

        i. a prossecução do cumprimento, da sua autorização ou de outras obrigações previstas na Diretiva 2013/36/UE, no Regulamento (UE) n.º 575/2013, na Diretiva 2014/65/UE, na Diretiva (UE) n.º 2015/2366 e na Diretiva 2009/110/CE, bem como das suas obrigações regulamentares,

        ii. o seu desempenho financeiro, ou

        iii. a sua solidez ou a continuidade dos seus serviços e atividades bancárias e de pagamento;

    b. caso sejam subcontratadas tarefas operacionais de funções de controlo interno, a menos que a avaliação determine que a não prestação da função subcontratada ou a sua prestação indevida não teria um impacto negativo na eficácia da função de controlo interno;

    c. caso pretendam subcontratar funções de atividades bancárias ou de serviços de pagamento com uma dimensão que requeira autorização [17] de uma autoridade competente, conforme referido na secção 12.1.

30. No que respeita às instituições, deve ser dada especial atenção à avaliação do caráter essencial ou da importância das funções, caso a subcontratação seja relativa a funções relacionadas com funções críticas e linhas de negócio críticas, tal como definidas no artigo 2.º, n.º 1, pontos 35 e 36, da Diretiva 2014/59/UE [18] e identificadas pelas instituições através dos critérios

[16] Ver também o artigo 30.º do Regulamento Delegado (UE) 2017/565 da Comissão, de 25 de abril de 2016, que completa a Diretiva 2014/65/UE do Parlamento Europeu e do Conselho no que diz respeito aos requisitos em matéria de organização e às condições de exercício da atividade das empresas de investimento e aos conceitos definidos para efeitos da referida diretiva.

[17] Ver as atividades enumeradas no anexo I da Diretiva 2013/36/UE.

[18] Diretiva 2014/59/UE do Parlamento Europeu e do Conselho, de 15 de maio de 2014, que estabelece um enquadramento para a recuperação e a resolução de instituições de crédito e de empresas de investimento e que altera a Diretiva 82/891/CEE do Conselho, e as Diretivas 2001/24/CE, 2002/47/CE, 2004/25/CE, 2005/56/CE, 2007/36/CE,

estabelecidos nos artigos 6.º e 7.º do Regulamento Delegado (UE) 2016/778 da Comissão[19]. As funções que são necessárias para a execução das princjpais atividades de linhas de negócio críticas ou de funções críticas devem ser consideradas pelas instituições como funções essenciais ou importantes para efeitos das presentes orientações, a menos que a avaliação da instituição determine que a não prestação da função subcontratada ou a sua prestação indevida não teria um impacto adverso na continuidade operacional da atividade principal ou da função crítica.

31. Quando avaliam se um acordo de subcontratação está relacionado com uma função essencial ou importante, as instituições e as instituições de pagamento devem ter em conta, em conjunto com o resultado da avaliação dos riscos indicada na secção 12.2, pelo menos, os seguintes fatores:

    a. se o acordo de subcontratação está diretamente relacionado com a prestação de atividades bancárias ou de serviços de pagamento[20] para os quais estão autorizadas;

    b. o potencial impacto de qualquer interrupção da função subcontratada ou da incapacidade do prestador de serviços para prestar o serviço nos níveis de serviço acordados e de forma continuada, sobre:

        i. a resiliência e a viabilidade financeira a curto e longo prazo, incluindo, se aplicável, os seus ativos, fundos próprios, custos, financiamento, liquidez, proveitos e perdas,

        ii. a continuidade da atividade e a resiliência operacional,

        iii. o risco operacional, incluindo a conduta, as tecnologias de informação e de comunicação (TIC) e o risco legal,

        iv. o risco reputacional,

        v. se aplicável, os planos de recuperação e de resolução, as possibilidades de resolução e a continuidade operacional numa situação de intervenção rápida, de recuperação ou de resolução;

    c. o potencial impacto do acordo de subcontratação na sua capacidade para:

        i. identificar, monitorizar e gerir todos os riscos,

2011/35/CE, 2012/30/UE e 2013/36/UE e os Regulamentos (UE) n.º 1093/2010 e (UE) n.º 648/2012 do Parlamento Europeu e do Conselho (JO L 173, de 12.6.2014, p. 190).

[19] Regulamento Delegado (UE) 2016/778 da Comissão, de 2 de fevereiro de 2016, que complementa a Diretiva 2014/59/UE do Parlamento Europeu e do Conselho no que diz respeito às circunstâncias e às condições em que o pagamento de contribuições extraordinárias ex post pode ser total ou parcialmente suspenso, bem como aos critérios para a determinação das atividades, serviços e operações ligados às funções críticas e das linhas de negócio e serviços associados ligados às linhas de negócio críticas (JO L 131, de 20.5.2016, p. 41).

[20] Ver as atividades enumeradas no anexo I da Diretiva 2013/36/UE.

ii. cumprir todos os requisitos legais e regulamentares,

iii. realizar auditorias adequadas sobre a função subcontratada;

d. o potencial impacto nos serviços prestados aos seus clientes;

e. todos os acordos de subcontratação, a exposição agregada da instituição ou da instituição de pagamento sobre o mesmo prestador de serviços e o potencial impacto de acordos de subcontratação cumulativos na mesma área de atividade;

f. a dimensão e a complexidade de qualquer área de atividade afetada;

g. a possibilidade de o acordo de subcontratação proposto poder ser incrementado sem a substituição ou revisão do acordo subjacente;

h. a capacidade para transferir o acordo de subcontratação proposto para outro prestador de serviços, se necessário ou desejável, tanto contratualmente como na prática, incluindo os riscos estimados, os impedimentos à continuidade da atividade, os custos e o período de tempo para essa transferência («substituibilidade»);

i. a capacidade para reintegrar a função subcontratada na instituição ou na instituição de pagamento, se necessário ou desejável;

j. a proteção dos dados e o potencial impacto de uma violação da confidencialidade ou da incapacidade de assegurar a disponibilidade e a integridade dos dados na instituição ou na instituição de pagamento e dos seus clientes, incluindo, mas não limitado ao cumprimento do Regulamento (UE) 2016/679[21].

[21] 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).

Título III – Quadro de governo

5 Sistemas de governo sólidos e risco de terceiros

32. No âmbito da estrutura global de controlo interno[22], nomeadamente dos mecanismos de controlo interno[23], as instituições e as instituições de pagamento devem dispor de um quadro holístico de gestão dos riscos a nível institucional que abranja todas as linhas de negócio e unidades internas. No âmbito desse quadro, as instituições e as instituições de pagamento devem identificar e gerir todos os seus riscos, incluindo os riscos decorrentes de acordos celebrados com terceiros. O quadro de gestão dos riscos deve igualmente permitir que as instituições e as instituições de pagamento tomem decisões plenamente informadas sobre a tomada de risco e garantir que as medidas de gestão dos riscos são implementadas de forma adequada, nomeadamente no que respeita aos riscos cibernéticos[24].

33. As instituições e as instituições de pagamento, tendo em conta o princípio da proporcionalidade, em conformidade com o disposto na secção 1, devem identificar, avaliar, monitorizar e gerir todos os riscos decorrentes de acordos celebrados com terceiros aos quais estejam ou possam vir a estar expostos, independentemente de esses acordos serem ou não acordos de subcontratação. Os riscos, em especial os riscos operacionais, de todos os acordos celebrados com terceiros, incluindo os riscos referidos nos pontos 26 e 28, devem ser avaliados em conformidade com o disposto na secção 12.2.

34. As instituições e as instituições de pagamento devem assegurar que cumprem todos os requisitos do Regulamento (UE) 2016/679, nomeadamente no que respeita aos seus acordos com terceiros e de subcontratação.

6 Sistemas de governo sólidos e subcontratação

35. A subcontratação de funções não pode resultar na delegação das responsabilidades do órgão de administração. As instituições e as instituições de pagamento continuam a ser inteiramente responsáveis pelo cumprimento de todas as suas obrigações regulamentares, incluindo a capacidade para supervisionar a subcontratação de funções essenciais ou importantes.

36. O órgão de administração é sempre inteiramente responsável, pelo menos, pelo seguinte:

    a. garantir que a instituição ou a instituição de pagamento cumpre, em permanência, as condições que deve observar para manter a autorização, incluindo quaisquer condições impostas pela autoridade competente;

---

[22] As instituições devem consultar o título V das orientações da EBA sobre governo interno.

[23] Consultar igualmente o artigo 11.º da Diretiva 2015/2366 (DSP2).

[24] Ver também as orientações da EBA sobre a gestão dos riscos associados às TIC e à segurança (https://eba.europa.eu/-/eba-consults-on-guidelines-on-ict-and-security-risk-management) e os elementos fundamentais do G7 para a gestão dos riscos cibernéticos por terceiros no setor financeiro (https://ec.europa.eu/info/publications/g7-fundamental-elements-cybersecurity-financial-sector_en).

b. a organização interna da instituição ou da instituição de pagamento;

c. a identificação, avaliação e gestão de conflitos de interesses;

d. a definição das estratégias e das políticas da instituição ou da instituição de pagamento (p. ex., o modelo de negócio, a apetência pelo risco, o quadro de gestão dos riscos);

e. o controlo da gestão corrente da instituição ou da instituição de pagamento, incluindo a gestão de todos os riscos associados à subcontratação; e

f. a função de controlo do órgão de administração na sua função de supervisão, incluindo a supervisão e o acompanhamento do processo de tomada de decisão da gestão.

37. A subcontratação não deve reduzir os requisitos de adequação aplicáveis aos membros do órgão de administração de uma instituição, aos diretores, às pessoas responsáveis pela gestão da instituição de pagamento e aos titulares de funções essenciais. As instituições e as instituições de pagamento devem dispor das competências adequadas e de recursos suficientes e devidamente qualificados para assegurar a gestão e a supervisão adequadas dos acordos de subcontratação.

38. As instituições e as instituições de pagamento devem:

a. atribuir claramente as responsabilidades pela documentação, pela gestão e pelo controlo dos acordos de subcontratação;

b. afetar recursos suficientes para assegurar o cumprimento de todos os requisitos legais e regulamentares, incluindo as presentes orientações, bem como a documentação e o acompanhamento de todos os acordos de subcontratação;

c. tendo em conta o disposto na secção 1 das presentes orientações, criar uma função de subcontratação ou nomear um quadro superior que seja diretamente responsável perante o órgão de administração (p. ex., um titular de uma função essencial de controlo) e responsável pela gestão e supervisão dos riscos decorrentes dos acordos de subcontratação, no âmbito da estrutura de controlo interno da instituição, e pela supervisão da documentação dos acordos de subcontratação. As instituições ou as instituições de pagamento de pequena dimensão e menos complexas devem, pelo menos, assegurar uma divisão clara das tarefas e responsabilidades em matéria de gestão e controlo dos acordos de subcontratação e podem atribuir a função de subcontratação a um membro do órgão de administração da instituição ou da instituição de pagamento.

39. As instituições e as instituições de pagamento devem manter permanentemente com «substância» suficiente e não se tornarem entidades vazias «*empty shells*» ou entidades destituídas de objeto «letter box entities». Para o efeito, devem:

a. cumprir permanentemente todas as condições da sua autorização [25], incluindo o desempenho efetivo das responsabilidades do órgão de administração, tal como definido no ponto 36 das presentes orientações;

b. manter um quadro organizativo e uma estrutura claros e transparentes que lhes permitam assegurar o cumprimento dos requisitos legais e regulamentares;

c. sempre que sejam subcontratadas tarefas operacionais das funções de controlo interno (p. ex., no caso de subcontratação intragrupo ou de subcontratação dentro de sistemas de proteção institucional), exercer uma supervisão adequada e ser capazes de gerir os riscos decorrentes da subcontratação de funções essenciais ou importantes; e

d. dispor de recursos e capacidades suficientes para assegurar o cumprimento das alíneas a), b) e c).

40. Nos processos de subcontratação, as instituições e as instituições de pagamento devem, pelo menos, assegurar que:

a. podem tomar e implementar decisões relacionadas com as suas atividades de negócio e as suas funções essenciais ou importantes, nomeadamente no que respeita àquelas que foram subcontratadas;

b. mantêm a regularidade do exercício da sua atividade e dos serviços bancários e de pagamento que prestam;

c. os riscos decorrentes dos acordos de subcontratação atuais e planeados são adequadamente identificados, avaliados, geridos e mitigados, incluindo os riscos relacionados com as TIC e a tecnologia financeira («fintech»);

d. são implementados acordos de confidencialidade adequados no que respeita a dados e a outras informações;

e. mantêm um fluxo adequado de informações relevantes com os prestadores de serviços;

f. no que respeita à subcontratação de funções essenciais ou importantes, podem realizar, pelo menos, uma das seguintes ações, num período de tempo adequado:

[25] Ver também as normas técnicas de regulamentação (NTR), nos termos do artigo 8.º, n.º 2, da Diretiva 2013/36/UE, sobre as informações a prestar para a autorização das instituições de crédito, e as normas técnicas de execução (NTI), nos termos do artigo 8.º, n.º 3, da mesma diretiva, sobre os formulários, modelos e procedimentos normalizados aplicáveis ao fornecimento das informações exigidas para a autorização das instituições de crédito (https://eba.europa.eu/regulation-and-policy/other-topics/rts-and-its-on-the-authorisation-of-credit-institutions).

No que respeita às instituições de pagamento, consultar as orientações da EBA relativas às informações a prestar para a autorização das instituições de pagamento e das instituições de moeda eletrónica e para o registo dos prestadores de serviços de informação sobre contas ao abrigo da Diretiva (UE) 2015/2366 (DSP2) (https://eba.europa.eu/documents/10180/2015792/Guidelines+on+Authorisations+of+Payment+Institutions+%28EBA-GL-2017-09%29_PT.pdf/c8a6dd92-8cf6-4b5e-b58f-090df4fc9b4e).

i. transferir a função para prestadores de serviços alternativos,

ii. reintegrar a função,

iii. descontinuar as atividades de negócio que dependam da função;

g. sempre que sejam tratados dados pessoais por prestadores de serviços localizados na UE e/ou em países terceiros, sejam implementadas medidas adequadas e os dados sejam tratados em conformidade com o Regulamento (UE) 2016/679.

7 Política de subcontratação

41. O órgão de administração de uma instituição ou de uma instituição de pagamento[26] que tenha celebrado acordos de subcontratação ou planeie celebrar tais acordos deve aprovar, rever regularmente e atualizar uma política de subcontratação reduzida a escrito e garantir a sua implementação, consoante aplicável, em base individual, subconsolidada e consolidada. No que respeita às instituições, a política de subcontratação deve observar as disposições da secção 8 das Orientações da EBA sobre governo interno e, em especial, ter em conta os requisitos estabelecidos na secção 18 (novos produtos e alterações significativas) dessas orientações. As instituições de pagamento também podem harmonizar as suas políticas com as disposições das secções 8 e 18 dessas orientações.

42. A política deve incluir as principais fases do ciclo de vida de um acordo de subcontratação e definir os princípios, as responsabilidades e os processos em matéria de subcontratação. Em especial, a política deve abranger, pelo menos:

a. as responsabilidades do órgão de administração em consonância com o ponto 36, incluindo a sua participação, se for caso disso, no processo de tomada de decisão de subcontratação de funções essenciais ou importantes;

b. a participação das linhas de negócio, funções de controlo interno e outras pessoas singulares no que respeita aos acordos de subcontratação;

c. o planeamento dos acordos de subcontratação, nomeadamente:

i. a definição dos requisitos de negócio relativos aos acordos de subcontratação,

ii. os critérios, incluindo os referidos na secção 4, e os processos para a identificação das funções essenciais ou importantes,

iii. a identificação, a avaliação e a gestão dos riscos, em conformidade com a secção 12.2,

[26] Ver também as orientações da EBA sobre medidas de segurança para gerir os riscos operacionais e de segurança dos serviços de pagamento ao abrigo da DSP2, disponíveis em: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2

iv. exame prévio («due diligence») dos potenciais prestadores de serviços, incluindo as medidas previstas na secção 12.3,

v. procedimentos para a identificação, avaliação, gestão e mitigação de potenciais conflitos de interesses, em conformidade com a secção 8,

vi. o planeamento da continuidade da atividade, em conformidade com a secção 9,

vii. o processo de aprovação de novos acordos de subcontratação;

d. a implementação, o acompanhamento e a gestão dos acordos de subcontratação, nomeadamente:

i. a avaliação contínua do desempenho do prestador de serviços, em conformidade com a secção 14,

ii. os procedimentos de notificação e de resposta a alterações a um acordo de subcontratação ou num prestador de serviços (p. ex., da sua situação financeira, da sua estrutura organizativa ou de propriedade, subcontratação em cadeia),

iii. a avaliação e a auditoria independentes do cumprimento dos requisitos legais e regulamentares e das políticas,

iv. os processos de renovação;

e. a documentação e a manutenção de registos, tendo em conta os requisitos da secção 11;

f. as estratégias de saída e os processos de rescisão, incluindo a obrigatoriedade de um plano de saída documentado para cada função essencial ou importante a subcontratar sempre que tal saída seja considerada possível, tendo em conta eventuais interrupções do serviço ou a rescisão de um acordo de subcontratação sem aviso prévio.

43. A política de subcontratação deve estabelecer distinção entre:

a. a subcontratação de funções essenciais ou importantes e outros acordos de subcontratação;

b. a subcontratação a prestadores de serviços autorizados por uma autoridade competente e a subcontratação a prestadores de serviços não autorizados;

c. acordos de subcontratação intragrupo, acordos de subcontratação no âmbito do mesmo sistema de proteção institucional (incluindo as entidades integralmente

detidas, individual ou coletivamente, por instituições do mesmo sistema de proteção institucional) e a subcontratação a entidades não pertencentes ao grupo; e

d. a subcontratação a prestadores de serviços localizados num Estado-Membro e em países terceiros.

44. As instituições e as instituições de pagamento devem assegurar que a política abrange a identificação dos seguintes efeitos potenciais de acordos de subcontratação de funções essenciais ou importantes e que estes são tidos em conta no processo de tomada de decisão:

a. o perfil de risco da instituição;

b. a capacidade para supervisionar o prestador de serviços e para gerir os riscos;

c. as medidas de continuidade da atividade; e

d. o desempenho das suas atividades de negócio.

8 Conflitos de interesses

45. As instituições, em conformidade com o título IV, secção 11, das Orientações da EBA sobre governo interno[27], e as instituições de pagamento devem identificar, avaliar e gerir os conflitos de interesses decorrentes dos seus acordos de subcontratação.

46. Sempre que a subcontratação crie conflitos de interesses materiais, nomeadamente entre entidades dentro do mesmo grupo ou do mesmo sistema de proteção institucional, as instituições e as instituições de pagamento devem adotar medidas adequadas para gerir esses conflitos de interesses.

47. Quando as funções são asseguradas por um prestador de serviços que faça parte de um grupo, seja membro de um sistema de proteção institucional ou que seja detido pela instituição, pela instituição de pagamento, pelo grupo ou pelas instituições que sejam membros de um sistema de proteção institucional, as condições para o serviço subcontratado, incluindo as condições financeiras, devem ser estabelecidas em condições de plena concorrência. No entanto, para efeitos da fixação dos preços dos serviços, é possível incluir no cálculo as sinergias resultantes da prestação de serviços idênticos ou similares a várias instituições de um grupo ou de um sistema de proteção institucional, desde que o prestador de serviços continue a ser viável numa base autónoma; no âmbito de um grupo, esta situação deve ser independente da incapacidade de qualquer outra entidade do grupo.

[27] As instituições de pagamento também podem harmonizar as suas políticas com essas orientações.

9 Planos de continuidade da atividade

48. As instituições, com base nos requisitos previstos no artigo 85.º, n.º 2, da Diretiva 2013/36/UE e no título VI das Orientações da EBA sobre governo interno[28], e as instituições de pagamento devem implementar, manter e testar periodicamente planos adequados de continuidade da atividade, no que respeita às funções essenciais ou importantes subcontratadas. As instituições e as instituições de pagamento de um grupo ou de um sistema de proteção institucional podem recorrer a planos de continuidade da atividade estabelecidos a nível central, no que diz respeito às suas funções subcontratadas.

49. Os planos de continuidade da atividade devem ter em conta a possibilidade de a qualidade do desempenho da função essencial ou importante subcontratada se deteriorar para um nível inaceitável ou falhar. Esses planos devem também ter em conta o potencial impacto da insolvência ou de outros incumprimentos dos prestadores de serviços e, se for caso disso, os riscos políticos na jurisdição do prestador de serviços.

10 Função de auditoria interna

50. As atividades da função de auditoria interna[29] devem, seguindo uma abordagem baseada no risco, abranger a avaliação independente das atividades subcontratadas. O programa e o plano de auditoria [30] devem incluir, nomeadamente, os acordos de subcontratação de funções essenciais ou importantes.

51. No que respeita ao processo de subcontratação, a função de auditoria interna deve, pelo menos, verificar:

    a. que o quadro da instituição ou da instituição de pagamento em matéria de subcontratação, incluindo a política de subcontratação, é implementado de forma correta e efetiva e cumpre a legislação e a regulamentação aplicáveis, a estratégia de risco e as decisões do órgão de administração;

    b. a adequação, a qualidade e a eficácia da avaliação do caráter essencial ou da importância das funções;

---

[28] Disponíveis em: https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised-

[29] No que respeita às responsabilidades da função de auditoria interna, as instituições devem consultar a secção 22 das orientações EBA sobre governo interno (https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised-) e as instituições de pagamento devem consultar a orientação n.º 5 das orientações da EBA sobre a autorização das instituições de pagamento (https://eba.europa.eu/documents/10180/2015792/Guidelines+on+Authorisations+of+Payment+Institutions+%28EBA-GL-2017-09%29_PT.pdf/c8a6dd92-8cf6-4b5e-b58f-090df4fc9b4e).

[30] Ver também as orientações da EBA relativas ao processo de revisão e avaliação pelo supervisor: https://eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2/guidelines-for-common-procedures-and-methodologies-for-the-supervisory-review-and-evaluation-process-srep-and-supervisory-stress-testing

c. a adequação, a qualidade e a eficácia da avaliação dos riscos decorrentes dos acordos de subcontratação, e se os riscos se mantêm em consonância com a estratégia de risco da instituição;

d. o envolvimento adequado dos órgãos de governo; e

e. o acompanhamento e a gestão adequados dos acordos de subcontratação.

11 Requisitos em matéria de documentação

52. No âmbito do respetivo quadro de gestão dos riscos, as instituições e as instituições de pagamento devem manter um registo atualizado de informações sobre todos os acordos de subcontratação existentes na instituição e, se for caso disso, em base subconsolidada e consolidada, conforme previsto na secção 2. Devem também documentar adequadamente todos os acordos de subcontratação em vigor, fazendo a distinção entre a subcontratação de funções essenciais ou importantes e outros acordos de subcontratação. Tendo em conta o direito nacional, as instituições devem conservar no registo a documentação dos acordos de subcontratação terminados, bem como a documentação de suporte, durante um período adequado.

53. Tendo em conta o título I das presentes orientações, e nas condições previstas no ponto 23, alínea d), no caso das instituições e das instituições de pagamento de um grupo, das instituições que estejam filiadas de modo permanente num organismo central ou das instituições que sejam membros do mesmo sistema de proteção institucional, o registo pode ser conservado centralmente.

54. O registo deve incluir, pelo menos, as informações seguintes relativas a todos os acordos de subcontratação existentes:

a. um número de referência para cada acordo de subcontratação;

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 e à instituição ou à instituição de pagamento;

c. uma breve descrição da função subcontratada, incluindo os dados que são objeto de subcontratação e se foram ou não transferidos dados pessoais (p. ex., indicando «sim» ou «não» num campo de dados separado) ou se o seu tratamento foi subcontratado a um prestador de serviços;

d. uma categoria atribuída pela instituição ou pela instituição de pagamento que reflita a natureza da função descrita na alínea c) (p. ex., função de controlo de tecnologias da informação), a qual deve facilitar a identificação dos diferentes tipos de acordos;

e. o nome do prestador de serviços, o número de registo da sociedade, o identificador da entidade jurídica (se existir), a morada da sede social e outras informações de contacto pertinentes, bem como o nome da empresa-mãe (se for caso disso);

f. o país ou países em que será desempenhado o serviço, incluindo a localização (ou seja, país ou região) dos dados;

g. se a função subcontratada é considerada (sim/não) essencial ou importante, incluindo, se for caso disso, um breve resumo dos motivos pelos quais a função subcontratada é considerada essencial ou importante;

h. no caso de subcontratação a um prestador de serviços de computação em nuvem, 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;

i. a data da avaliação mais recente do caráter essencial ou da importância da função subcontratada.

55. No que respeita à subcontratação de funções essenciais ou importantes, o registo deve incluir, pelo menos, as seguintes informações adicionais:

a. as instituições, as instituições de pagamento e outras empresas abrangidas pelo âmbito da consolidação prudencial ou do sistema de proteção institucional, se aplicável, que recorrem à subcontratação;

b. se o prestador de serviços ou o subprestador de serviços faz ou não parte do grupo, é membro do sistema de proteção institucional, ou é detido por instituições ou instituições de pagamento do grupo ou é detido por membros de um sistema de proteção institucional;

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

d. o órgão individual ou decisório (p. ex., o órgão de administração) da instituição ou da instituição de pagamento que aprovou o acordo de subcontratação;

e. a lei aplicável que rege o acordo de subcontratação;

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

g. se for caso disso, os nomes dos subcontratantes aos quais sejam subcontratadas partes significativas de uma função 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, o local (ou seja, país ou região) em que os dados serão armazenados;

h. o resultado da avaliação da substituibilidade do prestador de serviços (fácil, difícil ou impossível), da possibilidade de reintegração de uma função essencial ou importante na instituição ou na instituição de pagamento ou do impacto da interrupção da função essencial ou importante;

i. a identificação de prestadores de serviços alternativos, em conformidade com a alínea h);

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

k. o custo anual orçamentado estimado.

56. As instituições e as instituições de pagamento devem, mediante pedido, disponibilizar à autoridade competente o registo completo de todos os acordos de subcontratação existentes[31] ou secções específicas dos mesmos, tais como informações sobre todos os acordos de subcontratação abrangidos por uma das categorias a que se refere o ponto 54, alínea d), das presentes orientações (p. ex., todos os acordos de subcontratação de TI). As instituições e as instituições de pagamento devem facultar estas informações em formato eletrónico processável (p. ex., um formato de base de dados comum, valores separados por vírgulas).

57. As instituições e as instituições de pagamento devem, mediante pedido, disponibilizar à autoridade competente todas as informações necessárias para permitir que esta efetue uma supervisão efetiva da instituição ou da instituição de pagamento, incluindo, quando necessário, uma cópia do acordo de subcontratação.

58. Sem prejuízo do disposto no artigo 19.º, n.º 6, da Diretiva (UE) 2015/2366, as instituições e as instituições de pagamento devem informar as autoridades competentes, de forma adequada e em tempo útil, ou encetar um diálogo de supervisão com as autoridades competentes sobre a subcontratação planeada de funções essenciais ou importantes e/ou nos casos em que uma função subcontratada se tenha tornado essencial ou importante e disponibilizar, pelo menos, as informações especificadas no ponto 54.

59. As instituições e as instituições de pagamento[32] devem informar as autoridades competentes, de forma adequada e em tempo útil, de quaisquer alterações significativas e/ou acontecimentos graves relativos aos seus acordos de subcontratação suscetíveis de terem um impacto significativo na continuidade das atividades de negócio das instituições ou das instituições de pagamento.

60. As instituições e as instituições de pagamento devem documentar de forma adequada as avaliações efetuadas no âmbito do título IV, bem como os resultados do seu acompanhamento

[31] Consultar também as orientações da EBA relativas ao processo de revisão e avaliação pelo supervisor, disponíveis no seguinte endereço: https://eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2

[32] Ver também as orientações da EBA sobre a comunicação de incidentes de caráter severo, ao abrigo da Diretiva DSP2, disponíveis no seguinte endereço: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-major-incidents-reporting-under-psd2

contínuo (p. ex., desempenho do prestador de serviços, cumprimento dos níveis de serviço acordados, outros requisitos contratuais e regulamentares, atualizações da avaliação dos riscos).

Título IV – Processo de subcontratação

12 Análise prévia à subcontratação

61. Antes de celebrarem qualquer acordo de subcontratação, as instituições e as instituições de pagamento devem:

    a. avaliar se o acordo de subcontratação diz respeito a uma função essencial ou importante, conforme estabelecido no Título II;

    b. avaliar se são cumpridas as condições de supervisão para a subcontratação definidas na secção 12.1;

    c. identificar e avaliar todos os riscos relevantes do acordo de subcontratação, em conformidade com a secção 12.2;

    d. aplicar a diligência devida adequada ao potencial prestador de serviços, em conformidade com a secção 12.3;

    e. identificar e avaliar os conflitos de interesses que a subcontratação pode implicar, em conformidade com a secção 8.

12.1 Condições de supervisão da subcontratação

62. As instituições e as instituições de pagamento devem assegurar que a subcontratação de funções de atividades bancárias[33] ou de serviços de pagamento a um prestador de serviços localizado no mesmo ou noutro Estado-Membro, desde que o desempenho dessas funções exija uma autorização ou o registo por uma autoridade competente no Estado-Membro em que estão autorizadas, só seja realizada se for observada uma das seguintes condições:

    a. o prestador de serviços esteja autorizado ou registado por uma autoridade competente para o exercício de tais atividades bancárias ou serviços de pagamento; ou

    b. o prestador de serviços esteja autorizado a exercer tais atividades bancárias ou serviços de pagamento em conformidade com o quadro jurídico nacional aplicável.

63. As instituições e as instituições de pagamento devem assegurar que a subcontratação de funções de atividades bancárias ou de serviços de pagamento a um prestador de serviços

[33] Ver o artigo 9.º da Diretiva 2013/36/UE (DRFP) no que diz respeito à proibição de pessoas ou empresas que não sejam instituições de crédito exercerem a atividade de aceitação do público de depósitos ou outros fundos reembolsáveis.

localizado num país terceiro, desde que o desempenho dessas funções exija uma autorização ou o registo por uma autoridade competente no Estado-Membro em que estão autorizadas, só seja realizada se forem satisfeitas as seguintes condições:

a. o prestador de serviços esteja autorizado ou registado para a prestação dessa atividade bancária ou serviço de pagamento no país terceiro e esteja sujeito à supervisão de uma autoridade competente nesse país terceiro (designada por «autoridade de supervisão»);

b. exista um acordo de cooperação adequado, p. ex., sob a forma de um memorando de entendimento ou acordo colegial, entre as autoridades competentes responsáveis pela supervisão da instituição e as autoridades de supervisão responsáveis pela supervisão do prestador de serviços; e

c. o acordo de cooperação a que se refere a alínea b) deve assegurar que as autoridades competentes possam, pelo menos:

i. obter, mediante pedido, as informações necessárias para o desempenho das suas funções de supervisão decorrentes da Diretiva 2013/36/UE, do Regulamento (UE) n.º 575/2013, da Diretiva (UE) 2015/2366 e da Diretiva 2009/110/CE,

ii. obter, no país terceiro, acesso adequado a quaisquer dados, documentos, instalações ou pessoal que sejam relevantes para o exercício dos seus poderes de supervisão,

iii. receber, o mais rapidamente possível, informações da autoridade de supervisão do país terceiro para efeitos de investigação de infrações aparentes aos requisitos da Diretiva 2013/36/UE, do Regulamento (UE) n.º 575/2013, da Diretiva (UE) 2015/2366 e da Diretiva 2009/110/CE, e

iv. cooperar com as autoridades de supervisão competentes do país terceiro em matéria de execução, em caso de violação dos requisitos regulamentares e do direito nacional aplicáveis no Estado-Membro. A cooperação deve incluir, mas não deve ser limitada à a receção de informações das autoridades de supervisão do país terceiro sobre eventuais violações dos requisitos regulamentares aplicáveis, logo que tal seja praticável.

12.2 Avaliação dos riscos dos acordos de subcontratação

64. As instituições e as instituições de pagamento devem avaliar o potencial impacto dos acordos de subcontratação no seu risco operacional, ter em conta os resultados da avaliação na decisão de subcontratar a função a um prestador de serviços e devem adotar as medidas adequadas para evitar riscos operacionais acrescidos indevidos antes de celebrarem acordos de subcontratação.

65. A avaliação deve incluir, se for caso disso, cenários de possíveis eventos de risco, incluindo eventos de elevado risco operacional. No âmbito da análise de cenários, as instituições e as instituições de pagamento devem avaliar o impacto potencial de serviços não prestados ou inadequados, incluindo os riscos causados por processos, sistemas, pessoas ou acontecimentos externos. As instituições e as instituições de pagamento, tendo em conta o princípio da proporcionalidade a que se refere a secção 1, devem documentar a análise realizada e os seus resultados e estimar em que medida o acordo de subcontratação aumentaria ou diminuiria o seu risco operacional. Tendo em conta o disposto no título I, as instituições e as instituições de pagamento de pequena dimensão e não complexas podem utilizar métodos de avaliação qualitativa dos riscos, enquanto as instituições de grande dimensão e complexas devem adotar uma abordagem mais sofisticada, incluindo, se for caso disso, a utilização de dados internos e externos sobre perdas para fundamentar a análise de cenários.

66. No âmbito da avaliação dos riscos, as instituições e as instituições de pagamento devem igualmente ter em conta os benefícios e os custos esperados do proposto acordo de subcontratação proposto, incluindo a ponderação de quaisquer riscos que possam ser reduzidos ou ser objeto de melhor gestão face a quaisquer riscos que possam resultar do acordo de subcontratação proposto, tendo em conta, pelo menos:

    a. os riscos de concentração, incluindo os riscos decorrentes:

        i. da subcontratação a um prestador de serviços dominante que não seja facilmente substituível, e

        ii. de múltiplos acordos de subcontratação com o mesmo prestador de serviços ou com prestadores de serviços estreitamente ligados;

    b. os riscos agregados resultantes da subcontratação de várias funções em toda a instituição ou instituição de pagamento e, no caso de grupos de instituições ou de sistemas de proteção institucional, os riscos agregados em base consolidada ou com base no sistema de proteção institucional:

    c. no caso de instituições significativas, o risco de «step-in», ou seja, o risco que pode resultar da necessidade de prestar apoio financeiro a um prestador de serviços em dificuldade ou de assumir as suas operações de negócio; e

d. as medidas aplicadas pela instituição ou instituição de pagamento e pelo prestador de serviços para gerir e atenuar os riscos.

67. Sempre que o acordo de subcontratação inclua a possibilidade de o prestador de serviços subcontratar em cadeia funções essenciais ou importantes a outros prestadores de serviços, as instituições e as instituições de pagamento devem ter em conta:

a. os riscos associados à subcontratação em cadeia, incluindo os riscos adicionais que podem surgir se o subcontratante estiver localizado num país terceiro ou num país diferente do do prestador de serviços;

b. o risco de que cadeias de subcontratação longas e complexas reduzam a capacidade das instituições ou das instituições de pagamento para acompanharem a função essencial ou importante subcontratada e a capacidade das autoridades competentes para supervisioná-las de forma efetiva.

68. Quando realizam a avaliação dos riscos antes da subcontratação e durante o acompanhamento permanente do desempenho do prestador de serviços, as instituições e as instituições de pagamento devem, pelo menos:

a. identificar e classificar as funções relevantes e os dados e sistemas associados, no que respeita à sua sensibilidade e medidas de segurança necessárias;

b. realizar uma análise rigorosa, baseada no risco, das funções e dos dados e sistemas associados cuja subcontratação está a ser ponderada ou que tenham sido subcontratados e lidar com os potenciais riscos, nomeadamente os riscos operacionais, incluindo o risco legal, das TIC, de conformidade e de reputação, e as limitações de supervisão relacionadas com os países onde se encontram os serviços subcontratados ou onde for provável que sejam fornecidos e onde os dados se encontram ou seja provável que estejam armazenados;

c. avaliar as consequências da localização do prestador de serviços (dentro ou fora da UE);

d. avaliar a situação de estabilidade política e de segurança das jurisdições em causa, incluindo:

i. as leis em vigor, incluindo as leis sobre proteção de dados,

ii. as disposições de aplicação coerciva das leis em vigor, e

iii. 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 instituição ou da instituição de pagamento, em especial;

e. definir e decidir um nível adequado de proteção da confidencialidade dos dados, de continuidade das atividades subcontratadas e da integridade e rastreabilidade dos dados e sistemas no contexto da subcontratação pretendida. As instituições e as instituições de pagamento devem ainda 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;

f. determinar se o prestador de serviços é uma filial ou uma empresa-mãe da instituição, é abrangido pelo âmbito da consolidação contabilística ou é membro ou propriedade de instituições que sejam membros de um sistema de proteção institucional e, em caso afirmativo, em que medida a instituição controla o prestador de serviços ou tem capacidade para influenciar as suas ações em conformidade com a secção 2.

12.3 Exame prévio («Due diligence»)

69. No seu processo de seleção e avaliação, as instituições e as instituições de pagamento, antes de celebrarem um acordo de subcontratação e de avaliarem os riscos operacionais relacionados com a função a subcontratar, devem certificar-se de que o prestador de serviços é adequado.

70. No que respeita às funções essenciais e importantes, as instituições e as instituições de pagamento devem certificar-se de que o prestador de serviços possui a reputação comercial, as competências adequadas e suficientes, os conhecimentos especializados, a capacidade, os recursos (p. ex., humanos, de TI, financeiros), a estrutura organizativa e, se for caso disso, a ou as autorizações e o ou os registos regulamentares exigidos para desempenhar a função essencial ou importante de uma forma fiável e profissional que lhe permita cumprir as suas obrigações durante o período de vigência do contrato.

71. Os fatores adicionais a ter em conta na condução do exame prévio em relação a um potencial prestador de serviços devem incluir, mas não estar limitados ao seguinte:

a. o seu modelo de negócio, natureza, nível, complexidade, situação financeira, estrutura de grupo e de propriedade;

b. as relações a longo prazo com prestadores de serviços que já tenham sido avaliados e prestem serviços à instituição ou à instituição de pagamento;

c. se o prestador de serviços é uma empresa-mãe ou uma filial da instituição ou da instituição de pagamento, faz parte do âmbito da consolidação contabilística da instituição ou é membro ou propriedade de instituições que sejam membros do mesmo sistema de proteção institucional a que a instituição pertence;

d. se o prestador de serviços é ou não objeto de supervisão pelas autoridades competentes.

72. Sempre que a subcontratação implique o tratamento de dados pessoais ou confidenciais, as instituições e as instituições de pagamento devem certificar-se de que o prestador de serviços aplica medidas técnicas e organizativas adequadas para proteger esses dados.

73. As instituições e as instituições de pagamento devem adotar medidas adequadas para garantir que os prestadores de serviços atuam de uma forma coerente com os seus valores e o seu código de conduta. Em especial, no que respeita aos prestadores de serviços localizados em países terceiros e, se aplicável, aos seus subcontratantes, as instituições e as instituições de pagamento devem certificar-se de que o prestador de serviços atua de uma forma responsável do ponto de vista social e ético e respeita as normas internacionais em matéria de direitos humanos (p. ex., a Convenção Europeia dos Direitos do Homem), proteção do ambiente e condições de trabalho adequadas, incluindo a proibição do trabalho infantil.

13 Fase contratual

74. Os direitos e obrigações da instituição, da instituição de pagamento e do prestador de serviços devem ser claramente identificados e especificados num acordo por escrito.

75. O acordo de subcontratação de funções essenciais ou importantes deve estabelecer, pelo menos:

    a. uma descrição clara da função subcontratada a ser prestada;

    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 e à instituição ou à instituição de pagamento;

    c. a lei aplicável que rege o acordo;

    d. as obrigações financeiras das partes;

    e. se é permitida a subcontratação em cadeia de uma função essencial ou importante, ou de partes significativas da mesma, e, em caso afirmativo, as condições especificadas na secção 13.1 que a subcontratação em cadeia deve observar;

    f. o local ou os locais (ou seja, regiões ou países) em que a função essencial ou importante será prestada e/ou em que os dados relevantes serão mantidos e tratados, incluindo o possível local de armazenamento, e as condições a cumprir, nomeadamente, a obrigação de notificar a instituição ou a instituição de pagamento se o prestador de serviços propuser a alteração do ou dos locais;

    g. se for caso disso, disposições relativas à acessibilidade, disponibilidade, integridade, privacidade e segurança dos dados relevantes, conforme especificado na secção 13.2;

    h. o direito de a instituição ou a instituição de pagamento acompanhar permanentemente o desempenho do prestador de serviços;

i. os níveis de serviço acordados, que devem incluir objetivos de desempenho quantitativos e qualitativos concretos para a função subcontratada, 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 à instituição ou à instituição de pagamento, incluindo a comunicação, pelo prestador de serviços, de qualquer desenvolvimento suscetível de ter um impacto material na capacidade do prestador de serviços para desempenhar de forma eficiente a função essencial ou importante em consonância com os níveis de serviço acordados e em conformidade com a legislação e os requisitos regulamentares aplicáveis e, se for caso disso, a obrigação do prestador de serviços de apresentar relatórios da sua função de auditoria interna;

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

l. os requisitos de implementação e teste dos planos de contingência;

m. disposições que assegurem o acesso aos dados detidos pela instituição ou pela instituição de pagamento em caso de insolvência, resolução ou interrupção das operações de negócio do prestador de serviços;

n. a obrigação de o prestador de serviços cooperar com as autoridades competentes e as autoridades de resolução da instituição ou da instituição de pagamento, incluindo outras pessoas por elas designadas;

o. no caso das instituições, uma referência clara aos poderes da autoridade nacional de resolução, nomeadamente aos artigos 68.º e 71.º da Diretiva 2014/59/UE (DRRB) e, em especial, uma descrição das «obrigações substantivas» do contrato, na aceção do artigo 68.º dessa Diretiva;

p. o direito ilimitado das instituições, das instituições de pagamento e das autoridades competentes de inspecionar e auditar o prestador de serviços no que diz respeito, em especial, à função essencial ou importante objeto de subcontratação, conforme especificado na secção 13.3;

q. direitos de rescisão, conforme especificado na secção 13.4.

13.1 Subcontratação em cadeia de funções essenciais ou importantes

76. O acordo de subcontratação deve especificar se é ou não autorizada a subcontratação em cadeia de funções essenciais ou importantes ou de partes significativas das mesmas.

77. Se a subcontratação em cadeia de funções essenciais ou importantes for autorizada, as instituições e as instituições de pagamento devem determinar se a parte da função que será objeto de subcontratação em cadeia é, enquanto tal, essencial ou importante (ou seja, uma parte significativa da função essencial ou importante) e, em caso afirmativo, inscrevê-la no registo.

78. Se a subcontratação em cadeia de funções essenciais ou importantes for autorizada, o acordo por escrito deve:

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

    b. especificar as condições a respeitar em caso de subcontratação em cadeia;

    c. especificar que o prestador de serviços é obrigado a supervisionar os serviços que subcontratou em cadeia, a fim de assegurar o cumprimento permanente de todas as obrigações contratuais entre o prestador de serviços e a instituição ou a instituição de pagamento;

    d. exigir que o prestador de serviços obtenha previamente e por escrito, autorização específica ou geral da instituição ou da instituição de pagamento antes da subcontratação em cadeia dos dados[34];

    e. incluir a obrigação de o prestador de serviços informar a instituição ou a instituição de pagamento de qualquer subcontratação em cadeia prevista, ou de qualquer alteração significativa da mesma, em especial, se for suscetível de afetar a capacidade do prestador de serviços de cumprirem com as suas responsabilidades no âmbito do acordo de subcontratação. Tal inclui as alterações significativas previstas dos subcontratantes em cadeia e do período de notificação. Em especial, o período de notificação a ser definido deve permitir que a instituição ou a instituição de pagamento subcontratante, pelo menos, realize uma avaliação dos riscos das alterações propostas e se oponha a alterações antes da entrada em vigor da subcontratação em cadeia prevista ou de alterações significativas da mesma;

    f. assegurar, se for caso disso, que a instituição ou a instituição de pagamento tem o direito de se opor à subcontratação em cadeia prevista ou a alterações significativas da mesma, ou que é exigida uma aprovação explícita;

    g. assegurar que a instituição ou a instituição de pagamento tem o direito contratual de rescindir o contrato em caso de subcontratação em cadeia indevida, p. ex., se a subcontratação em cadeia aumentar significativamente os riscos para a instituição ou a instituição de pagamento ou se o prestador de serviços proceder à subcontratação em cadeia sem notificar a instituição ou a instituição de pagamento.

[34] Ver o artigo 28.º do Regulamento (UE) 2016/679.

79. As instituições e as instituições de pagamento só devem aceitar a subcontratação em cadeia se o subcontratante em cadeia assumir o compromisso de:

    a. cumprir integralmente a legislação, os requisitos regulamentares e as obrigações contratuais aplicáveis; e

    b. conceder à instituição, à instituição de pagamento e à autoridade competente os mesmos direitos contratuais de acesso e auditoria concedidos pelo prestador de serviços.

80. As instituições e as instituições de pagamento devem assegurar que o prestador de serviços efetua uma supervisão adequada dos prestadores de serviços em cadeia, em consonância com a política definida pela instituição ou pela instituição de pagamento. Se a subcontratação em cadeia proposta for suscetível de ter efeitos adversos materiais no acordo de subcontratação de uma função essencial ou importante ou de conduzir a um aumento material do risco, nomeadamente se as condições previstas no ponto 79 não forem cumpridas, a instituição ou a instituição de pagamento deve exercer o seu direito de oposição à subcontratação em cadeia, caso esse direito tenha sido acordado, e/ou de rescindir o contrato.

13.2 Segurança dos dados e dos sistemas

81. As instituições e as instituições de pagamento devem assegurar que os prestadores de serviços, se for caso disso, cumprem normas adequadas em matéria de segurança informática.

82. Se for caso disso (p. ex., no contexto de subcontratação de serviços de computação em nuvem ou de outros serviços de TIC), as instituições e as instituições de pagamento devem definir os requisitos de segurança dos dados e dos sistemas no âmbito do acordo de subcontratação e monitorizar o seu cumprimento de forma permanente.

83. No caso de subcontratação a prestadores de serviços de computação em nuvem e de outros acordos de subcontratação que impliquem o tratamento ou a transferência de dados pessoais ou confidenciais, as instituições e as instituições de pagamento devem adotar uma abordagem baseada no risco no que respeita ao local ou locais de armazenamento e de tratamento dos dados (ou seja, país ou região), bem como considerações em matéria de segurança da informação.

84. Sem prejuízo dos requisitos do Regulamento (UE) 2016/679, as instituições e as instituições de pagamento devem ter em conta, nos processos de subcontratação (em especial, a países terceiros), as diferenças nas disposições nacionais relativas à proteção de dados. As instituições e as instituições de pagamento devem assegurar que o acordo de subcontratação inclui a obrigação de o prestador de serviços proteger informações confidenciais, pessoais ou que sejam sensíveis por outras razões e cumprir todos os requisitos legais em matéria de proteção de dados aplicáveis à instituição ou à instituição de pagamento (p. ex., os direitos em matéria de proteção de dados pessoais e a observância do sigilo bancário ou de outros deveres legais de confidencialidade similares com respeito à informação de clientes, se aplicável).

13.3 Direitos de acesso, informação e auditoria

85. As instituições e as instituições de pagamento devem assegurar, no âmbito do acordo de subcontratação por escrito, que a função de auditoria interna é capaz de avaliar a função subcontratada, utilizando uma abordagem baseada no risco.

86. Independentemente do caráter essencial ou da importância das funções subcontratadas, os acordos de subcontratação por escrito entre instituições e prestadores de serviços devem fazer referência aos poderes de recolha de informações e de investigação das autoridades competentes e das autoridades de resolução nos termos do artigo 63.º, n.º 1, alínea a), da Diretiva 2014/59/UE e do artigo 65.º, n.º 3, da Diretiva 2013/36/UE, no que respeita aos prestadores de serviços localizados num Estado-Membro, e devem ainda assegurar esses direitos relativamente aos prestadores de serviços localizados em países terceiros.

87. No que respeita à subcontratação de funções essenciais ou importantes, as instituições e as instituições de pagamento devem assegurar, no âmbito do acordo de subcontratação por escrito, que o prestador de serviços lhes concede e às suas autoridades competentes, incluindo as autoridades de resolução, bem como a quaisquer outras pessoas designadas pelas mesmas ou pelas autoridades competentes, os seguintes direitos:

    a. pleno acesso a todas as instalações comerciais relevantes (p. ex., 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 («direitos de acesso e de informação»); e

    b. direitos ilimitados de inspeção e auditoria relacionados com o acordo de subcontratação («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.

88. No que respeita à subcontratação de funções que não sejam essenciais ou importantes, as instituições e as instituições de pagamento devem assegurar os direitos de acesso e auditoria previstos no ponto 87, alíneas a) e b), e na secção 13.3, segundo uma abordagem baseada no risco, tendo em conta a natureza da função subcontratada e o risco operacional e reputacional conexo, o seu caráter redimensionável, o impacto potencial na continuidade do desempenho das suas atividades e o período contratual. As instituições e as instituições de pagamento devem ter em conta que as funções podem tornar-se essenciais ou importantes com o decorrer do tempo.

89. As instituições e as instituições de pagamento devem assegurar que o acordo de subcontratação ou qualquer outro acordo contratual não impeça ou limite o exercício efetivo dos direitos de acesso e de auditoria por parte das mesmas, das autoridades competentes ou de terceiros designados pelas mesmas para exercer esses direitos.

90. As instituições e as instituições de pagamento devem exercer os seus direitos de acesso e de auditoria, determinar a frequência das auditorias e os domínios a auditar, segundo uma abordagem baseada no risco, e respeitar as normas de auditorias nacionais e internacionais pertinentes e geralmente aceites[35].

91. Sem prejuízo da sua responsabilidade final relativamente aos acordos de subcontratação, as instituições e as instituições de pagamento podem utilizar:

    a. auditorias comuns organizadas conjuntamente com outros clientes do mesmo prestador de serviços e realizadas por si e por esses clientes ou por terceiros por si designados, a fim de utilizarem os recursos de auditoria com maior eficiência e reduzirem os encargos administrativos para os clientes e para o prestador de serviços;

    b. certificações de terceiros e relatórios de auditoria interna ou de terceiros disponibilizados pelo prestador de serviços.

92. No que respeita à subcontratação de funções essenciais ou importantes, as instituições e as instituições de pagamento devem avaliar se os relatórios e as certificações de terceiros a que se refere o ponto 91, alínea b), são adequados e suficientes para cumprirem as suas obrigações regulamentares, e não devem, ao longo do tempo, recorrer exclusivamente a esses relatórios.

93. As instituições e as instituições de pagamento só devem utilizar o método a que refere o ponto 91, alínea b), se:

    a. concordarem com o plano de auditoria para a função subcontratada;

    b. assegurarem que o âmbito da certificação ou do relatório de auditoria abrange os sistemas (ou seja, processos, aplicações, infraestruturas, centros de dados, etc.) e os controlos chave identificados pela instituição ou pela instituição de pagamento, bem como o cumprimento dos requisitos regulamentares aplicáveis;

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

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

    e. tiverem confirmado a aptidão da entidade de certificação ou de auditoria (p. ex., no que se refere à rotatividade da empresa de certificação ou de auditoria, qualificações, conhecimentos especializados, repetição/verificação das evidências no ficheiro de auditoria subjacente);

[35] No que concerne às instituições, consultar a secção 22 das orientações da EBA sobre governo interno: https://eba.europa.eu/documents/10180/2164689/Guidelines+on+Internal+Governance+%28EBA-GL-2017-11%29_PT.pdf

f. tiverem a certeza de que as certificações são emitidas e as auditorias são realizadas de acordo com normas profissionais relevantes amplamente reconhecidas e incluem um teste da eficácia operacional dos controlos chave implementados;

g. 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; e

h. mantiverem o direito contratual de realizar auditorias individuais, por sua livre iniciativa, no que respeita à subcontratação de funções essenciais ou importantes.

94. Em conformidade com as Orientações da EBA relativas à avaliação do risco das TIC no âmbito do processo de revisão e avaliação pelo supervisor (SREP), as instituições devem, se for caso disso, certificar-se de que são capazes de realizar testes de penetração de segurança para avaliar a efetividade das medidas e processos de cibersegurança e de segurança interna das TIC[36] implementadas. Tendo em conta o disposto no título I, as instituições de pagamento devem igualmente dispor de mecanismos internos de controlo das TIC, incluindo medidas de controlo da sua segurança e de mitigação dos seus riscos.

95. Antes de uma visita ao local planeada, as instituições, as instituições de pagamento, as autoridades competentes e os auditores ou terceiros que atuem em nome da instituição, da instituição de pagamento ou das autoridades competentes devem notificar o prestador de serviços com uma antecedência razoável, a menos que tal não seja possível devido a uma situação de emergência ou de crise ou que conduza a uma situação em que a auditoria já não seja efetiva.

96. Ao realizar auditorias em ambientes com vários clientes, devem ser tomadas precauções para evitar ou mitigar os riscos para o ambiente de outro cliente (p. ex., impacto nos níveis de serviço, disponibilidade de dados, questões de confidencialidade).

97. Nos casos em que o acordo de subcontratação implique um elevado nível de complexidade técnica, por exemplo, no caso de subcontratação de serviços de computação em nuvem, a instituição ou a instituição de pagamento deve verificar se as pessoas que realizam a auditoria (sejam os seus auditores internos, o conjunto de auditores ou auditores externos agindo em seu nome) possuem as competências e os conhecimentos adequados para realizar as auditorias e/ou as avaliações relevantes de forma efetiva. O mesmo é aplicável a qualquer membro do pessoal da instituição ou da instituição de pagamento que avalie auditorias ou certificações de terceiros realizadas por prestadores de serviços.

[36] Ver também as orientações da EBA relativas à avaliação do risco das TIC: https://eba.europa.eu/documents/10180/1954038/Guidelines+on+ICT+Risk+Assessment+under+SREP+%28EBA-GL-2017-05%29_PT.pdf/94b1a29e-d5d2-496a-ab04-58c11f3cee83

13.4 Direitos de rescisão

98. O acordo de subcontratação deve expressamente permitir a sua rescisão pela instituição ou instituição de pagamento em conformidade com a legislação aplicável, nomeadamente nas seguintes situações:

    a. se o prestador que assegura as funções subcontratadas infringir a legislação, a regulamentação ou as disposições contratuais aplicáveis;

    b. se forem identificados impedimentos suscetíveis de alterar o desempenho da função subcontratada;

    c. se existirem alterações materiais que afetem o acordo de subcontratação ou o prestador de serviços (p. ex., subcontratação em cadeia ou alterações de subcontratantes em cadeia);

    d. se existirem insuficiências no que diz respeito à gestão e à segurança de dados ou informações que sejam confidenciais, pessoais ou sensíveis por outras razões; e

    e. se forem dadas instruções pela autoridade competente da instituição ou da instituição de pagamento, p. ex., no caso de a autoridade competente, devido ao acordo de subcontratação, já não estar em condições de supervisionar eficazmente a instituição ou a instituição de pagamento.

99. O acordo de subcontratação deve facilitar a transferência da função subcontratada para outro prestador de serviços ou a sua reintegração na instituição ou na instituição de pagamento. Para o efeito, o acordo de subcontratação por escrito deve:

    a. especificar claramente as obrigações do atual prestador de serviços em caso de transferência da função subcontratada para outro prestador de serviços ou para a instituição ou instituição de pagamento, incluindo o tratamento de dados;

    b. definir um período de transição adequado durante o qual o prestador de serviços, após a rescisão do acordo de subcontratação, deverá continuar a assegurar a função subcontratada a fim de reduzir o risco de interrupções; e

    c. incluir a obrigação de o prestador de serviços apoiar a instituição ou a instituição de pagamento na transferência ordenada da função em caso de rescisão do acordo de subcontratação.

14 Supervisão das funções subcontratadas

100. As instituições e as instituições de pagamento devem acompanhar permanentemente o desempenho dos prestadores de serviços em relação a todos os acordos de subcontratação, segundo uma abordagem baseada no risco, prestando especial atenção à subcontratação de funções essenciais ou importantes, incluindo a garantia da disponibilidade, da integridade e da segurança dos dados e informações. Nos casos em que o risco, a natureza ou o nível de uma função subcontratada se tenha alterado significativamente, as instituições e as instituições de pagamento devem reavaliar o caráter essencial ou a importância dessa função, em conformidade com a secção 4.

101. As instituições e as instituições de pagamento devem aplicar a devida competência, zelo e diligência aquando do acompanhamento e da gestão dos acordos de subcontratação.

102. As instituições devem atualizar regularmente a sua avaliação dos riscos em conformidade com a secção 12.2 e devem informar periodicamente o órgão de administração sobre os riscos identificados no que respeita à subcontratação de funções essenciais ou importantes.

103. As instituições e as instituições de pagamento devem acompanhar e gerir os seus riscos de concentração interna decorrentes de acordos de subcontratação, tendo em conta a secção 12.2 das presentes orientações.

104. As instituições e as instituições de pagamento devem assegurar, de forma permanente, que os acordos de subcontratação (e colocando a tónica nas funções essenciais ou importantes subcontratadas) cumprem normas adequadas em matéria de desempenho e qualidade em consonância com as suas políticas, mediante:

a. a garantia de que recebem relatórios adequados dos prestadores de serviços;

b. a avaliação do desempenho dos prestadores de serviços, utilizando ferramentas como indicadores chave de desempenho, indicadores de controlos chave, relatórios de prestação de serviços, autocertificação e análises independentes; e

c. a análise de todas as restantes informações relevantes recebidas do prestador de serviços, incluindo testes e relatórios sobre medidas de continuidade da atividade e.

105. As instituições devem tomar as medidas adequadas, caso identifiquem deficiências na prestação da função subcontratada. Em especial, as instituições e as instituições de pagamento devem dar seguimento a quaisquer indicações de que os prestadores de serviços não estão a desempenhar as funções essenciais ou importantes subcontratadas de forma efetiva ou em conformidade com a legislação e os requisitos regulamentares aplicáveis. Se forem identificadas deficiências, as instituições e as instituições de pagamento devem adotar medidas corretivas apropriadas, as quais podem incluir a rescisão do acordo de subcontratação, com efeito imediato, se necessário.

15 Estratégias de saída

106. Quando procedem à subcontratação de funções essenciais ou importantes, as instituições e as instituições de pagamento devem dispor de uma estratégia de saída devidamente documentada que esteja em consonância com a política de subcontratação e os planos de continuidade da atividade[37], tendo em conta, pelo menos, a possibilidade de:

a. rescisão de acordos de subcontratação;

b. incumprimento do prestador de serviços;

c. deterioração da qualidade da função subcontratada prestada e de interrupção real ou potencial da atividade causada pela inadequada ou falha na prestação da função;

d. riscos materiais para o desempenho adequado e continuado da função.

107. As instituições e as instituições de pagamento devem assegurar que estão em condições de abandonar os acordos de subcontratação sem qualquer interrupção indevida das suas atividades de negócio, sem limitar o seu cumprimento dos requisitos regulamentares e sem prejuízo da continuidade e da qualidade da sua prestação de serviços aos clientes. Para o efeito, devem:

a. elaborar e implementar planos de saída abrangentes, documentados e, se for caso disso, suficientemente testados (p. ex., através da realização de uma análise dos potenciais custos, impactos, recursos e implicações em termos da calendarização da transferência de um serviço subcontratado para um prestador alternativo); e

b. identificar soluções alternativas e elaborar planos de transição que permitam à instituição ou à instituição de pagamento eliminar as funções e os dados subcontratados no prestador de serviços e transferi-los para prestadores alternativos ou devolvê-los à instituição ou à instituição de pagamento, ou adotar outras medidas que garantam a continuidade da prestação da função essencial ou importante ou da atividade de negócio de uma forma controlada e suficientemente testada, tendo em conta os desafios que possam surgir devido à localização dos dados e adotando as medidas necessárias para assegurar a continuidade da atividade durante a fase de transição.

108. Quando elaboram estratégias de saída, as instituições e as instituições de pagamento devem:

a. definir os objetivos da estratégia de saída;

[37] As instituições, em conformidade com os requisitos previstos no artigo 85.º, n.º 2, da Diretiva 2013/36/UE e no título VI das orientações da EBA sobre governo interno, e as instituições de pagamento devem dispor de planos de continuidade da atividade adequados no que respeita à subcontratação de funções essenciais ou importantes.

b. realizar uma análise do impacto das atividades de negócio que seja proporcional ao risco dos processos, serviços ou atividades objeto de subcontratação, com o objetivo de identificar quer os recursos humanos e financeiros que seriam necessários para executar o plano de saída quer o tempo necessário para essa execução;

c. atribuir funções, responsabilidades e recursos suficientes para gerir os planos de saída e a transição das atividades;

d. definir critérios de êxito para a transição das funções e dos dados subcontratados; e

e. definir os indicadores a utilizar para o acompanhamento do acordo de subcontratação (conforme descrito na secção 14), incluindo indicadores baseados em níveis de serviço inaceitáveis que deverão desencadear a saída.

Título V – Orientações relativas à subcontratação destinadas às autoridades competentes

109. Quando estabelecem métodos adequados para o controlo da conformidade das instituições e das instituições de pagamento com as condições da autorização inicial, as autoridades competentes devem procurar identificar se os acordos de subcontratação implicam uma alteração significativa das condições e obrigações da autorização inicial das instituições e das instituições de pagamento.

110. As autoridades competentes devem certificar-se de que podem supervisionar efetivamente as instituições e as instituições de pagamento, incluindo aquelas que tenham assegurado, nos seus acordos de subcontratação, que os prestadores de serviços são obrigados a conceder direitos de auditoria e de acesso à autoridade competente e à instituição, em conformidade com a secção 13.3.

111. A análise dos riscos de subcontratação das instituições deve ser realizada, pelo menos, no âmbito do processo de revisão e avaliação pelo supervisor (SREP) ou, no que concerne às instituições de pagamento, no âmbito de outros processos de supervisão, incluindo pedidos ad hoc, ou durante inspeções no local.

112. Além das informações inscritas no registo, conforme referido na secção 11, as autoridades competentes podem solicitar informações adicionais às instituições e às instituições de pagamento, em especial no que respeita a acordos de subcontratação essenciais ou importantes, tais como:

a. a análise dos riscos detalhada;

b. se o prestador de serviços possui um plano de continuidade da atividade adequado para os serviços prestados à instituição ou instituição de pagamento que procede à subcontratação;

c. a estratégia de saída a utilizar em caso de rescisão do acordo de subcontratação por uma das partes ou em caso de interrupção na prestação dos serviços; e

d. os recursos e as medidas implementadas para acompanhar adequadamente as atividades subcontratadas.

113. Além das informações exigidas na secção 11, as autoridades competentes podem exigir que as instituições e as instituições de pagamento forneçam informações pormenorizadas sobre qualquer acordo de subcontratação, mesmo que a função em causa não seja considerada essencial ou importante.

114. As autoridades competentes devem avaliar o seguinte, segundo uma abordagem baseada no risco:

a. se as instituições e as instituições de pagamento acompanham e gerem adequadamente, em especial, os acordos de subcontratação de funções essenciais ou importantes;

b. se as instituições e as instituições de pagamento dispõem de recursos suficientes para acompanharem e gerirem os acordos de subcontratação;

c. se as instituições e as instituições de pagamento identificam e gerem todos os riscos relevantes; e

d. se as instituições e as instituições de pagamento identificam, avaliam e gerem adequadamente os conflitos de interesses no que respeita aos acordos de subcontratação, p. ex., no caso de subcontratação intragrupo ou de subcontratação dentro do mesmo sistema de proteção institucional.

115. As autoridades competentes devem assegurar que todas as instituições e instituições de pagamento da UE/EEE não funcionam como «conchas vazias», incluindo situações em que as instituições utilizam operações de compra e venda recíproca («back-to-back») ou operações intragrupo para transferir parte do risco de mercado e do risco de crédito para uma entidade não pertencente à UE/ao EEE, e devem assegurar que dispõem de mecanismos adequados de governo e de gestão dos riscos para identificarem e gerirem os seus riscos.

116. Na sua avaliação, as autoridades competentes devem ter em conta todos os riscos, nomeadamente[38]:

a. os riscos operacionais[39] decorrentes do acordo de subcontratação;

[38] No que respeita às instituições abrangidas pela Diretiva 2013/36/UE, ver também as orientações da EBA relativas ao processo de revisão e avaliação pelo supervisor (SREP): https://eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2

[39] Ver também as orientações da EBA relativas ao risco das TIC: https://eba.europa.eu/documents/10180/1954038/Guidelines+on+ICT+Risk+Assessment+under+SREP+%28EBA-GL-2017-05%29_PT.pdf/94b1a29e-d5d2-496a-ab04-58c11f3cee83

b. o risco reputacional;

c. o risco de «step-in» que pode obrigar a instituição a resgatar um prestador de serviços, no caso de instituições significativas;

d. os riscos de concentração no seio da instituição, incluindo em base consolidada, causados por vários acordos de subcontratação com um único prestador de serviços ou com prestadores de serviços estreitamente ligados entre si, ou por vários acordos de subcontratação no mesmo domínio de atividade;

e. os riscos de concentração a nível setorial, p. ex., quando várias instituições ou instituições de pagamento utilizam um único prestador de serviços ou um pequeno grupo de prestadores de serviços;

f. a medida em que a instituição ou a instituição de pagamento que efetua a subcontratação controla o prestador de serviços ou tem capacidade para influenciar as suas ações, a redução dos riscos que pode resultar de um nível de controlo mais elevado e se o prestador de serviços está incluído na supervisão consolidada do grupo; e

g. os conflitos de interesses entre a instituição e o prestador de serviços.

117. Sempre que sejam identificados riscos de concentração, as autoridades competentes devem acompanhar a evolução desses riscos e avaliar quer o seu impacto potencial noutras instituições e instituições de pagamento quer a estabilidade do mercado financeiro; as autoridades competentes devem, se for caso disso, informar a autoridade de resolução sobre novas funções potencialmente essenciais [40] que tenham sido identificadas durante esta avaliação.

118. Sempre que sejam identificadas preocupações que permitam concluir que uma instituição ou uma instituição de pagamento já não dispõe de mecanismos de governo sólidos ou não cumpre os requisitos regulamentares, as autoridades competentes devem adotar medidas adequadas, que podem incluir 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 a instituição ou a instituição de pagamento funcionar em permanência, a anulação de contratos pode ser necessária, caso não seja possível assegurar a supervisão e a aplicação coerciva dos requisitos regulamentares através de outras medidas.

119. As autoridades competentes devem certificar-se de que têm condições para exercer uma supervisão efetiva, em especial, quando as instituições e as instituições de pagamento subcontratam funções essenciais ou importantes que são desempenhadas fora da UE/EEE.

[40] Na aceção do artigo 2.º, n.º 1, ponto 35, da Diretiva DRRB.