ЭЛЕКТРОННЫЕ ДЕНЬГИ

Руководство Европейской Службы по банковскому надзору (EBA) по аутсорсингу*

АПРЕЛЬ 2023

Ассоциация участников рынка электронных денег и денежных переводов «АЭД» - отраслевая ассоциация, созданная в 2010 году.

Ассоциация является широко признанным центром компетенции по платежам, специализированному финансовому регулированию, повышению доступности финансовых услуг и финансовым инновациям как в России, так и за рубежом. Основные задачи АЭД – устойчивое развитие отрасли, распространение лучших деловых практик и оказание экспертной поддержки для государственных органов и частного сектора.

Сайт Ассоциации: www.npaed.ru,

Электронная почта: npaed@npaed.ru

Телеграмм-канал «Записки на рукавах» - здесь мы обсуждаем новации в платежном секторе и регулировании, рассуждаем о будущем платежей, финтеха и криптовалют.

Будем рады видеть новых подписчиков!

EBA Guidelines on outsourcing arrangements
25 February 2019
EBA/GL/2019/02

Оглавление

Введение

Цифровизация финансового сектора сильно повлияла на бизнес финансовых организаций. Они все больше передают различные функции третьим сторонам: поддержку инфраструктуры, хранение некоторых типов данных, разработку мобильных приложений, и многие другие. Сторонние компании помогают участникам рынка и в соблюдении регулятивных требований: например, составлении отчетности, проведении проверок клиентов. Из консервативных учреждений банки становятся больше похожи на ИТ-компании, для которых такой аутсорсинг привычен.

Для регулятора эта тенденция тревожна. Когда банк передает какие-то функции на аутсорсинг, он становится неизбежно зависим от стороннего поставщика услуг, который может не подпадать ни под какое регулирование. Риски не сводятся к чисто технологическим. Если сторонний поставщик услуг работает по праву другого государства, то у банка возникает слишком много неизвестных переменных, и корректно спрогнозировать возможные проблемы может быть затруднительно.

Перед вами – неофициальный перевод Руководства Европейской Службы по банковскому надзору по аутсорсингу. Это в определенной степени модельный нормативный акт, который регулирует вопросы аутсорсинга в финансовом секторе. Руководство одновременно и предельно конкретно, и в то же время дает участникам рынка самостоятельно определять меры по минимизации рисков или определению круга критических функций. Оно также затрагивает очень специфичные темы: к примеру, субаутсорсинг, страновые риски, проблему «стратегии выхода».

Прямое копирование иностранного опыта редко оказывается удачным. Однако, по нашему мнению, для русскоязычной аудитории Руководство могло бы быть интересным пособием по проблематике аутсорсинга в целом и отправной точкой в дискуссиях между регулятором и частным сектором. Наконец, для участников рынка это еще неплохой ориентир для проведения инвентаризации внутренних процессов и процедур, связанных с аутсорсингом.

Виктор Достов, председатель Совета Ассоциации участников рынка электронных денег и денежных переводов АЭД

Павел Шуст, исполнительный директор Ассоциации участников рынка электронных денег и денежных переводов АЭД

1. Комплаенс и требования к отчетности

Статус настоящего Руководства

1. Положения настоящего документа приняты на основании статьи 16 Регламента (ЕС) № 1093/2010[1]. В соответствии со статьей 16(3) Регламента (ЕС) № 1093/2010, компетентные органы и финансовые организации должны приложить все усилия для соблюдения настоящего Руководства.

2. Настоящее Руководство излагает позицию ЕВА о практике надзора в рамках Европейской системы финансового надзора, а также о правоприменительной практике ЕС в данной области. Компетентные органы в понимании статьи 4(2) Регламента (ЕС) № 1093/2010, к которым обращено настоящее Руководство, должны соблюдать положения настоящего документа, включив их, при необходимости, в свою практику (например, путем внесения изменений в законодательную базу или надзорные процессы), в том числе в тех случаях, когда положения Руководства направлены в первую очередь на финансовые организации и платежные учреждения.

Требования к отчетности

3. В соответствии со статьей 16(3) Регламента (ЕС) № 1093/2010, компетентные органы должны уведомить ЕВА о соблюдении (или таковом намерении) настоящего Руководство, или, в ином случае, указать причины его несоблюдения, до 31.12.2021[2]. В случае отсутствия какого-либо уведомления к этому сроку, компетентные органы будут рассматриваться ЕБА как не соответствующие требованиям. Для уведомления ЕВА необходимо заполнить форму, доступную на веб-сайте ЕВА, и направить ее по адресу compliance@eba.europa.eu с пометкой "EBA/GL/2019/02". Уведомления должны подаваться лицами, имеющими соответствующие полномочия. Любое изменение в статусе компетентного органа о его соответствии также должны быть доведены до сведения ЕВА.

4. Уведомления будут опубликованы на веб-сайте ЕВА в соответствии со статьей 16(3).

[1]Регламент N 1093/2010 Европейского парламента и Совета Европейского Союза "Об учреждении Европейского надзорного органа (Европейский банковский орган), об изменении Решения 716/2009/ЕС и об отмене Решения 2009/78/ЕС Европейской Комиссии" (Принят в г. Страсбурге 24.11.2010) (OJ L 331, 15.12.2010, стр. 12).

[2]В оригинале Руководства срок реализации оставлен пустым. Но позднее ЕВА зафиксировало его на 31.12.2021 г. – прим. пер.

2. Предмет, сфера применения и терминология

Предмет

5. Настоящее Руководство определяет принципы внутреннего управления, включая эффективное управление рисками, которыми финансовые организации, платежные учреждения и операторы электронных денег должны руководствоваться при передаче функций на аутсорсинг, в том числе при передаче на аутсорсинг существенных или критических функций.

6. Настоящее Руководство определяет подходы к осуществлению регулятивного надзора за исполнением указанных в предыдущем пункте принципов. Компетентные органы должны непрерывно контролировать соблюдение организациями условий выданных им разрешений на передачу функций на аутсорсинг, руководствуясь статьей 97 Директивы 2013/36/ЕС[3], системой SREP[4], статьей 9(3) Директивы ЕС 2015/2366[5] (Второй платежной Директивы[6]) и статьей 5(5) Директивы 2009/110/ЕС[7].

Адресаты

7. Настоящее Руководство адресовано компетентным органам, определенным в пункте 40 статьи 4(1) Регламента (ЕС) № 575/2013[8], включая Европейский центральный банк в отношении задач, возложенных на него Регламентом (ЕС) № 1024/2013[9], финансовым организациям, определенным в пункте 3 статьи 4(1) Регламента (ЕС) № 575/2013, платежным учреждениям, определенным в статье 4(4) Директивы (ЕС) 2015/2366, и операторам электронных денег, определенным статьей 2(1) Директивы 2009/110/ЕС. Провайдеры услуг по агрегации финансовой информации, оказывающие

[3]Директива N 2013/36/ЕС Европейского парламента и Совета Европейского Союза о доступе к осуществлению деятельности кредитными организациями и пруденциальном надзоре за кредитными организациями и инвестиционными компаниями, вносящая изменения в Директиву 2002/87/ЕС и отменяющая Директивы 2006/48/ЕС и 2006/49/ЕС.

[4]Supervisory review and evaluation process, регулярный процесс по оценке количественных и качественных характеристик деятельности и рисков финансовых учреждений по четырём основным направлениям (бизнес-модель и ее доходность, корпоративное управление и система управления рисками, риски для капитала, риски ликвидности) – прим. пер.

[5]Директива 2015/2366/ЕС Европейского парламента и Совета от 25 ноября 2015 года о платежных услугах на внутреннем рынке и о внесении изменений в Директивы 2002/65/ЕС, 2009/110/ЕС и 2013/36/ЕС и Регламент (ЕС) № 1093/2010 и об отмене Директивы 2007/64/ЕС.

[6]Неофициальный перевод Директивы доступен на сайте Ассоциации АЭД www.npaed.ru/analytics - прим. пер.

[7]Директива N 2009/110/ЕС Европейского парламента и Совета Европейского Союза об учреждении и деятельности организаций, эмитирующих электронные деньги, о пруденциальном надзоре за их деятельностью, а также об изменении Директив 2005/60/ЕС и 2006/48/ЕС и об отмене Директивы 2000/46/ЕС

[8]Регламент (ЕС) № 575/2013 Европейского парламента и Совета от 26 июня 2013 г. о пруденциальных требованиях к кредитным учреждениям и инвестиционным компаниям и об изменении Регламента (ЕС) № 646/2012 (OJ L 176, 27.6.2013, стр. 1) – прим. пер.

[9]Регламент (ЕС) Совета ЕС N 1024/2013 от 15 октября 2013 г. о возложении на Европейский Центральный Банк особых задач, касающихся пруденциального надзора за кредитными организациями – прим. пер.

только платежные услуги, упомянутые в пункте (8) Приложения I Директивы (ЕС) 2015/2366, не подпадают под действие настоящего Руководства в соответствии со статьей 33 упомянутой Директивы.

8. Для целей настоящего Руководства, под платежными учреждениями подразумеваются также операторы электронных денег, а платежные услуги включают в себя также услуги по выпуску электронных денег.

Область применения

9. Финансовые организации, определенные в пункте 3 статьи 3 (1) Директивы 2013/36/ЕС[10], подпадают под действие настоящего Руководства и должны соблюдать его положения на индивидуальной, субконсолидированной и консолидированной основе, если это не противоречит Директиве 2014/65/ЕС[11] и Постановления Комиссии (ЕС) 2017/565[12] (которое содержит требования в отношении аутсорсинга учреждениями, предоставляющими инвестиционные услуги и осуществляющими инвестиционную деятельность, а также соответствующие указания Европейского управления по ценным бумагам и рынкам в отношении инвестиций и инвестиционных услуг). Компетентные органы могут освободить организацию от соблюдения положений настоящего руководства на индивидуальной основе в соответствии со статьей 21 Директивы 2013/36/ЕС[13] или статьей 109(1) Директивы 2013/36/ЕС совместно со статьей 7 Регламента (ЕС) № 575/2013[14]. Финансовые организации, на которые распространяется действие Директивы 2013/36/ЕС, должны соблюдать данную Директиву и настоящее Руководство на консолидированной и субконсолидированной основе в соответствии со статьей 21 и статьями 108-110 Директивы 2013/36/ЕС.

10. Платежные учреждения и операторы электронных денег должны соблюдать положения настоящего Руководства на индивидуальной основе, если это не

[10] Кредитные организации (выдающие кредиты и принимающие депозиты) и инвестиционные фирмы – прим.пер.

[11] Директива N 2014/65/ЕС Европейского парламента и Совета Европейского Союза от 15 мая 2014 года о рынках финансовых инструментов и об изменении Директивы 2002/92/ЕС и Директивы 2011/61/ЕС (OJ L 173, 12.6.2014, стр. 349).

[12] Делегированный Регламент Европейской Комиссии (ЕС) 2017/565 от 25 апреля 2016 года, дополняющим Директиву Европейского Парламента и Европейского Совета 2014/65/ЕС относительно организационных требований к инвестиционным фирмам и условий деятельности, и дефиниций понятий для целей упомянутой Директивы (OJ L 87, 31.3.2017, стр. 1).

[13] Кредитные организации, которые на постоянной основе аффилированы с головной компанией – прим. пер.

[14] Случаи, когда на головную организацию и дочернюю организацию распространяются единые надзорные требования – с учетом условий, описанных в статье 7 Директивы 575/2013 – прим. пер.

противоречит статьи 8 (3) Директивы (ЕС) 2015/2366[15] и статье 5 (7) Директивы 2009/110/ЕС[16].

11. Компетентные органы, в чьи обязанности входит осуществление надзора за финансовыми организациями, платежными учреждениями и операторами электронных денег, должны руководствоваться положениями настоящего документа.

Термины и определения

12. Если не указано иное, термины, используемые и определяемые в Директиве 2013/36/ЕС, Регламенте (ЕС) № 575/2013, Директиве 2009/110/ЕС, Директиве (ЕС) 2015/2366 и Руководстве ЕВА по внутреннему управлению[17], имеют то же значение в настоящем Руководстве. Кроме того, для целей настоящего Руководства, применяются следующие термины:

Аутсорсинг	означает соглашение, заключенное в любой форме между финансовой организацией, платежным учреждением или оператором электронных денег и поставщиком услуг, на основании которого поставщик услуг берет на себя определенные процессы, операции, оказывает услуги или осуществляет деятельность, которые в противном случае осуществляла бы сама финансовая организация, платежное учреждение или оператор электронных денег.
Функция	означает любые процессы, услуги или деятельность.
Критическая или существенная функция[18]	означает любую функцию, которая считается критической или существенной, как указано в части 4 настоящего Руководства.
Субаутсорсинг	означает ситуацию, когда поставщик услуг в рамках соглашения об аутсорсинге в дальнейшем передает

[15]Исключение, позволяющее не рассчитывать размер собственных средств платежных институтов на индивидуальной основе, если они включены в консолидированный надзор головной кредитной организации – прим. пер.

[16]Исключение, позволяющее не рассчитывать размер собственных средств оператора системы электронных денег на индивидуальной основе, если они включены в консолидированный надзор головной кредитной организации – прим. пер.

[17]Руководстве ЕВА по внутреннему управлению (https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised-).

[18]Формулировка "критическая или существенная функция" основана на формулировке, используемой в соответствии с Директивой 2014/65/ЕС (MiFID II) и Делегированным Регламентом Европейской Комиссии 2017/565, дополняющим MiFID II, и используется только для целей аутсорсинга; она не связана с определением "критических функций" для целей механизмов восстановления и разрешения споров, определенный в статье 2(1)(35) Директивы 2014/59/ЕС (BRRD).

	вверенную ему на аутсорсинг функцию другому поставщику услуг[19].
Поставщик услуг	означает стороннюю организацию, которая частично или полностью берет на себя процесс, оказывает услугу или осуществляет деятельность, переданную ей на аутсорсинг в рамках соглашения об аутсорсинге.
Облачные сервисы	означает сервисы, предоставляемые с использованием облачных вычислительных ресурсов, обеспечивая таким образом повсеместный, удобный сетевой доступ к общему пулу конфигурируемых вычислительных ресурсов (например, к сетевому и серверному оборудованию, системам хранения данных, приложениям и услугам), которые могут быть быстро предоставлены с минимальными усилиями или с минимальным вмешательством со стороны поставщиков услуг.
Публичный облачный сервис	облачная инфраструктура, доступная для использования неопределенным кругом клиентов.
Частный облачный сервис	облачная инфраструктура, доступная только одной организации или платежному учреждению.
Общественный облачный сервис	облачная инфраструктура, доступная для определенной группы организаций или платежных учреждений, в том числе нескольких связанных между собой учреждений.
Гибридные облачные сервисы	облачная инфраструктура, состоящая из двух или более различных облачных инфраструктур.
Орган управления	орган (или органы) организации или платежного учреждения, назначающиеся в соответствии с национальным законодательством, которые уполномочены определять стратегию, цели и общее направление деятельности организации или платежного учреждения, и которые осуществляют надзор и контроль за принятием управленческих решений и включают лиц, которые фактически руководят бизнесом, а также директоров и лиц, ответственных за управление платежным учреждением.

[19] Для оценки применяются положения части 3; субаутсорсинг также упоминается в других документах EBA как "цепочка аутсорсинга" (‘chain of outsourcing’ или ‘chain-outsourcing’).

3. Особенности вступления в силу

Дата вступления в силу

13. Настоящее Руководство, за исключением пункта 63(b), вступает в силу 30 сентября 2019 года и применимо ко всем соглашениям об аутсорсинге, заключенным, пересмотренным или измененным в эту дату или после нее. Пункт 63(b) вступает в силу 31 декабря 2021 года.

14. Финансовые организации и платежные учреждения должны внести соответствующие изменения в действующие соглашения об аутсорсинге, чтобы они соответствовали положениям настоящего Руководства.

15. В случае, если пересмотр соглашений об аутсорсинге существенных или критических функций не будет завершен к 31 декабря 2021 года, финансовым организациям и платежным учреждениям необходимо проинформировать об этом компетентные органы, в том числе указать, какие шаги организация планирует предпринять для приведения соглашений в соответствие или какие существуют варианты расторжения соглашения об аутсорсинге.

Переходные положения

16. Финансовые организации и платежные учреждения должны привести в соответствие все существующие соглашения об аутсорсинге (за исключением соглашений об аутсорсинге с поставщиками облачных сервисов) с момента их продления, но не позднее 31 декабря 2021 года.

Прекращение действия ранее принятых положений

17. Положения Руководства Комитета европейских органов банковского надзора (CEBS) по аутсорсингу от 14 декабря 2006 года и рекомендации Европейского банковского управления (EBA) по аутсорсингу поставщикам облачных сервисов[20] отменяются с 30 сентября 2019 года.

[20]Рекомендации EBA по аутсорсингу поставщикам облачных услуг (EBA/REC/2017/03).

4. Особенности вступления в силу

Раздел I - Пропорциональность: применение группам компаний и схемы институциональной защиты

1 Пропорциональность

18. Финансовые организации, платежные учреждения и компетентные органы должны при соблюдении или надзоре за соблюдением положений настоящего Руководства учитывать принцип пропорциональности. Исходя из принципа пропорциональности, в целях повышения эффективности регулирования механизмы управления, в том числе связанные с аутсорсингом, должны соответствовать индивидуальному профилю риска, характеру и бизнес-модели финансовой организации или платежного учреждения.

19. Внедряя требования положений, изложенных в настоящем Руководстве, финансовые организации и платежные учреждения должны учитывать сложность передаваемых на аутсорсинг функций, связанные с этим риски, критичность или существенность передаваемых на аутсорсинг функций, и потенциальное влияние аутсорсинга на непрерывность деятельности.

20. Исходя из принципа пропорциональности, финансовые организации, платежные учреждения[21] и компетентные органы должны принимать во внимание критерии, указанные в разделе I Руководства EBA по внутреннему управлению в соответствии со статьей 74(2) Директивы 2013/36/ЕС.

2 Аутсорсинг деятельности групп компаний и финансовых организаций, которые являются членами институциональных систем защиты

21. В соответствии со статьей 109 (2) Директивы 2013/36/ЕС, положения настоящего Руководства должны также применяться на субконсолидированной и консолидированной основе, с учетом уровня консолидации[22]. Европейские головные компании или головные компании, находящиеся в государстве-члене ЕС[23], должны

[21]Платежным учреждениям также следует ознакомиться с Руководством EBA в рамках Второй платежной Директивы относительно информации, которая должна предоставляться для выдачи разрешения на ведение деятельности платежным учреждением и учреждением, эмитирующим электронные деньги, а также для регистрации провайдеров услуг по агрегации финансовой информации. Руководство доступно на сайте EBA: https://www.eba.europa.eu/regulation-and-policy/payment-services-

[22]Подробнее в подпунктах (47) и (48) пункта 1 статьи 4 Регламента (ЕС) № 575/2013 об уровне консолидации.

[23] В соответствии с Директивой 2013/36/ЕС, если в Европейском Союзе действуют несколько финансовых компаний, принадлежащих к иностранной группе, по достижении определенного размера общих активов (40 млрд. евро), то в ЕС для них должна быть создана головная компания-посредник. Этот посредник будет зарегистрирован в ЕС и напрямую подчиняться иностранной головной компании. Создание такой головной

обеспечить в дочерних компаниях последовательные, глубоко интегрированные и адекватные механизмы внутреннего управления и бизнес-процессов.

22. Финансовые организации и платежные учреждения, в соответствии с пунктом 21, и учреждения, которые выступают в качестве членов институциональных систем защиты и используют централизованные механизмы управления, должны соблюдать следующие положения:

    a) если финансовые организации или платежные учреждения заключают соглашения об аутсорсинге с поставщиками услуг в рамках группы компаний или институциональной системы защиты[24], то орган управления этих финансовых организаций или платежных учреждений несет полную ответственность за соблюдение всех нормативных требований и за эффективное применение положений настоящего Руководства, в том числе в отношении соглашений об аутсорсинге;

    b) если эти финансовые организации или платежные учреждения в рамках группы компаний или институциональной системы защиты передают операционную часть внутреннего контроля стороннему поставщику услуг, необходимо выработать механизмы оценки эффективности решений таких задач на аутсорсинге, в том числе путем получения соответствующих отчетов.

23. В дополнение к пункту 22, финансовые организации и платежные учреждения, осуществляющие свою деятельность в рамках группы компаний, за исключением случаев, подпадающих под статью 109 Директивы 2013/36/ЕС и статью 7 Регламента (ЕС) № 575/2013, а также финансовые организации, выступающие в роли головной компании группы или постоянно аффилированные с головной компанией группы, которым не предоставлены освобождения, предусмотренные статьей 21 Директивы 2013/36/ЕС, и финансовые организации, являющиеся членами институциональной системы защиты, должны учитывать следующее:

    a) если мониторинг аутсорсинга осуществляется централизованно (например, в рамках генерального соглашения о мониторинге деятельности, переданной на аутсорсинг), финансовые организации и платежные учреждения, как минимум для критических и важных функций, должны осуществлять мониторинг и в собственном качестве. Такой мониторинг должен включать получение, по крайней мере, ежегодно или по запросу, от организации, осуществляющей

компании-посредника позволяет европейским регулятором осуществлять консолидированный надзор за той частью группы, которая работает на территории ЕС.

[24] В соответствии со статьей 113(7) Регламента (ЕС) № 575/2013 (Capital Requirements Regulation; CRR), схема институциональной защиты означает договорное или установленное законом соглашение об ответственности, которое защищает участников схемы, и, в частности, обеспечивает их ликвидность и платежеспособность во избежание банкротства, если это необходимо.

централизованный мониторинг, отчетов, включающих как минимум резюме оценки рисков и эффективности деятельности аутсорсинговых компаний. Кроме того, финансовые организации и платежные учреждения должны получать от организации, осуществляющей централизованный мониторинг аутсорсинговой деятельности, резюме соответствующих аудиторских отчетов по аутсорсингу критических и существенных функций, а по запросу - полные версии таких отчетов;

b) для оценки влияния изменений в отношении поставщиков услуг, контроль за которыми осуществляется централизованно, финансовым организациям и платежным учреждениям необходимо должным образом информировать свое руководство о планируемых изменениях в отношении таких поставщиков услуг, о потенциальном влиянии этих изменений на критические или существенные функции, а также предоставить резюме анализа рисков, в том числе юридических, соответствия нормативным требованиям и влияния на качество предоставления услуг;

c) если финансовые организации и платежные учреждения, входящие в группу компаний, учреждения, аффилированные с головной компанией группы, или учреждения, являющиеся частью институциональной системы защиты, полагаются на централизованную оценку соглашений об аутсорсинге, как указано в части 12, то каждая финансовая организация и платежное учреждение должно получить резюме такой оценки и учитывать ее в контексте специфики своей бизнес-модели и возможных рисков;

d) если реестр всех существующих соглашений об аутсорсинге, как указано в части 11, создан и ведется централизованно в рамках группы компаний или институциональной системы защиты, компетентные органы, все финансовые организации и платежные институты должны иметь возможность получить доступ к необходимым данным из реестра в кратчайшие сроки. Этот реестр должен включать все соглашения об аутсорсинге, в том числе соглашения об аутсорсинге с поставщиками услуг внутри данной группы компаний или институциональной системы защиты;

e) если план выхода из соглашения об аутсорсинге критической или существенной функции разработан на уровне группы компаний, в рамках институциональной системы защиты или головной компанией группы, все финансовые организации и платежные учреждения должны получить краткое изложение этого плана и убедиться в том, что они смогут реализовать его на практике.

24. Головные компании, находящееся в стране-члене ЕС, а также их дочерние предприятия, головные компании и аффилированные лица должны выполнять положения настоящего Руководства, кроме случаев, подпадающих под действие стати 21 Директивы 2013/36/ЕС или статьи 109(1) Директивы 2013/36/ЕС совместно со статьей 7 Регламента (ЕС) № 575/2013[25].

25. Если головная компания находится на территории ЕС или зарегистрирована в ЕС и не подпадает под действие статьи 21 Директивы 2013/36/ЕС или статьи 109(1) Директивы 2013/36/ЕС и статьи 7 Регламента (ЕС) № 575/2013, то ее финансовые организации и платежные учреждения должны выполнять положения настоящего Руководства в собственном качестве.

Раздел II - Оценка соглашений об аутсорсинге

3 Аутсорсинг

26. Финансовые организации и платежные учреждения должны определить, подпадает ли соглашение с третьей стороной под понятие аутсорсинга. В частности, следует установить, выполняется ли функция (или ее часть), переданная на аутсорсинг поставщику услуг, на периодической или постоянной основе, а также выявить, могла ли и должна ли была эта финансовая организация или платежное учреждение самостоятельно выполнять переданную третьей стороне функцию (или ее часть), даже если ранее этим не занималась.

27. Если соглашение с поставщиком услуг охватывает несколько функций, финансовые организации и платежные учреждения должны учитывать это при оценке, например, если предоставляемая услуга включает предоставление оборудования для хранения данных и их резервное копирование, оба эти элемента должны рассматриваться в совокупности.

28. По общему правилу, к аутсорсингу не относятся:

    a. переданные третьим лицам функции, которые по закону должны выполняться поставщиком услуг, например, обязательный аудит;

    b. предоставление рыночной информации (например, предоставление данных Bloomberg, Moody's, Standard & Poor's, Fitch);

    c. доступ к глобальной инфраструктуре (например, Visa, MasterCard);

[25]Дополнительные исключения, предусмотренные для групп компаний, на которые распространяется консолидированный надзор, или когда дочерняя финансовая организация постоянно аффилирована с головной кредитной организацией – прим. пер.

d. клиринговые и расчетные соглашения между клиринговыми палатами, центральными контрагентами, расчетными учреждениями и их членами;

e. глобальные инфраструктуры обмена финансовыми сообщениями, которые подлежат надзору со стороны соответствующих органов;

f. корреспондентские банковские услуги; и

g. приобретение услуг, которые для финансовой организации или платежного учреждения не являются профильными (например, консультации архитектора, предоставление юридического заключения, представительство в суде и административных органах, уборка, озеленение и содержание помещений финансовой организации или платежного учреждения, медицинские услуги, обслуживание служебных автомобилей, питание, услуги торгового автомата, канцелярские услуги, туристические услуги, услуги почтового отделения, услуги секретаря и оператора коммутатора), товаров (например, пластиковые карты, считыватели карт, канцелярские принадлежности, персональные компьютеры, мебель) или коммунальных услуг (например, электричество, газ, вода, телефонная линия).

4 Существенные или критические функции

29. Функция всегда должна считаться существенной или критической, если[26]:

a. сбой в осуществлении такой функции может нанести значимый ущерб, в частности:

i. нарушение непрерывного соблюдения условий выданных финансовой организации или платежному учреждению разрешений, нормативных обязательств, а также других обязательств в соответствии с Директивой 2013/36/ЕС, Регламентом (ЕС) № 575/2013, Директивой 2014/65/ЕС, Директивой (ЕС) 2015/2366 и Директивой 2009/110/ЕС;

ii. ухудшение финансовых результатов; или

iii. нарушение устойчивого, непрерывного процесса предоставления банковских и платежных услуг и ведения деятельности.

b. на аутсорсинг передается операционная часть внутреннего контроля, за исключением случаев, при которых проведенная оценка показывает, что непредоставление или ненадлежащее выполнение этой функции третьей

[26]См. также статью 30 Делегированный Регламент Европейской Комиссии (ЕС) 2017/565 от 25 апреля 2016 года, дополняющим Директиву Европейского Парламента и Европейского Совета 2014/65/ЕС относительно организационных требований к инвестиционным фирмам и условий деятельности, и дефиниций понятий для целей упомянутой Директивы.

стороной не окажет негативного влияния на общую эффективность внутреннего контроля;

c. на аутсорсинг передаются функции, связанные с банковской деятельностью или с предоставлением платежных услуг в объеме, требующем разрешения[27] компетентного органа, как указано в части 12.1.

30. При заключении соглашений об аутсорсинге, финансовые организации должны уделить особое внимание оценке критичности и существенности функций, относящихся к основным направлениям деятельности, к критическим функциям, как определено[28] в статьях 2(1)(35) и 2(1)(36) Директивы 2014/59/ЕС[29], а также к другим критическим функциям, которые определила сама организация на основании критериев, изложенных в статьях 6 и 7 Постановления Комиссии (ЕС) 2016/778[30]. Для целей настоящего Руководства функции, необходимые для осуществления основных направлений бизнеса, а также другие критические функции, должны рассматриваться как критические или существенные, если только финансовая организация не установит, что отказ в предоставлении или ненадлежащее выполнение такой функции третьим лицом не окажет негативного влияния на операционную непрерывность основного бизнеса или другой критической функции.

31. При оценке критичности или существенности функции, передаваемой на аутсорсинг, финансовые организации и платежные учреждения, наряду с результатами оценки риска, изложенными в части 12.2, должны учитывать, по крайней мере, следующие факторы:

a. связано ли соглашение об аутсорсинге непосредственно с ведением той банковской деятельности или предоставлением тех платежных услуг[31], на которые им выдано разрешение;

---

[27]См. перечень видов деятельности в Приложении I к Директиве 2013/36/ЕС.

[28]Вкратце, к «критическим функциям» относятся те, которые критичны для реальной экономики, либо перебои в осуществлении которых могут привести к угрозам финансовой стабильности. «Основные направления деятельности» (core business lines) – деятельность, которая приносит финансовой организации существенную для нее прибыль – прим. пер.

[29]Директива 2014/59 /ЕС Европейского парламента и Совета от 15 мая 2014 года, регулирующая оздоровление кредитных учреждений и инвестиционных компаний и вносящая поправки в Директиву Совета 82/891/ЕЕС и Директивы 2001/24/ЕС, 2002/47/ЕС, 2004/25/ЕС, 2005/56/ЕС, 2007/36/ЕС, 2011/35/ЕС, 2012/30/ЕС и 2013/36/ЕС, а также Регламенты (ЕС) № 1093/2010 и (ЕС) № 648/2012 Европейского парламента и Совета (BRRD) (OJ L 173, 12.6.2014, стр. 190).

[30]Делегированный Регламент Европейской Комиссии (ЕС) 2016/778 от 2 февраля 2016 года, дополняющий Директиву 2014/59/ЕС Европейского парламента и Совета об обстоятельствах и условиях, при которых выплата чрезвычайных взносов ex post может быть частично или полностью отложена, а также критериев определения видов деятельности, услуг и операций в отношении критических функций, а также для определения направлений деятельности и связанных с ними услуг, относящихся к основным направлениям деятельности (OJ L 131, 20.5.2016, стр. 41).

[31]См. перечень видов деятельности в Приложении I к Директиве 2013/36/ЕС.

b. какое потенциальное воздействие может оказать сбой в выполнении функции, которая отдана на аутсорсинг, или неспособность третьей стороны оказывать на постоянной основе и качественно свои услуги на:

   i. краткосрочную и долгосрочную финансовую устойчивость и жизнеспособность, включая, если применимо, на активы, капитал, затраты, финансирование, ликвидность, прибыли и убытки;

   ii. непрерывность бизнеса и операционную устойчивость;

   iii. операционные риски, включая поведенческие, правовые риски и риски, связанные с информационно-коммуникационными технологиями (ИКТ);

   iv. репутационные риски;

   v. возможность осуществления плана по восстановлению деятельности и финансовой, операционной устойчивости, в том числе, когда требуется раннее вмешательство надзорных органов.

c. какое потенциальное влияние соглашение об аутсорсинге окажет на:

   i. выявление, контроль и управление всеми рисками;

   ii. соблюдение всех юридических и нормативных требований;

   iii. проведение соответствующих аудитов в отношении функций, переданных на аутсорсинг;

d. какое влияние передаваемая на аутсорсинг функция окажет на предоставляемые клиентам услуги;

e. воздействие на другие соглашения об аутсорсинге, потенциальная зависимость финансовой организации или платежного учреждения от одного поставщика услуг, а также потенциальное кумулятивное воздействие аутсорсинга на каждую отдельную область бизнеса;

f. масштаб и сложность части бизнеса, в которой будет использоваться аутсорсинг;

g. возможность расширения охвата соглашения об аутсорсинге без его замены или пересмотра;

h. возможность передачи соглашения об аутсорсинге другому поставщику услуг, если это необходимо или желательно, как по условиям договора, так и с практической точки зрения, включая оценку предполагаемых рисков,

связанных с непрерывностью ведения бизнеса, затрат и сроков ("заменяемость");

i. способность снова взять на себя ранее переданную на аутсорсинг функцию, если это необходимо или желательно;

j. надежность защиты данных, и как нарушение конфиденциальности или невозможность обеспечить доступность и целостность данных повлияет на финансовую организацию, платежное учреждение, клиентов, а также, помимо прочего, на соблюдение Регламента (ЕС) 2016/67939[32].

Раздел III - Система управления

5 Надлежащие механизмы управления и риски, связанные с третьими сторонами

32. В рамках общей системы внутреннего контроля[33], включая и механизмы внутреннего контроля[34], финансовые организации и платежные учреждения должны создать комплексную систему управления рисками, охватывающую все направления бизнеса и все внутренние подразделения. Финансовые организации и платежные учреждения должны выявлять все риски, включая риски, связанные с заключением соглашений с третьими сторонами, и управлять ими. В рамках системы управления рисками финансовые организации и платежные учреждения при принятии решения об аутсорсинге должны учитывать все риски, а также обеспечить меры по надлежащему управлению этими рисками, включая киберриски[35].

33. Финансовые организации и платежные учреждения, руководствуясь принципом пропорциональности в соответствии с частью 1, должны выявлять, оценивать, отслеживать и управлять всеми рисками, возникающими в результате заключения соглашений с третьими сторонами, которым они подвергаются или могут подвергнуться в будущем, независимо от того, являются ли эти соглашения соглашениями об аутсорсинге или нет. Все риски, и, в частности, операционные риски, связанные с любыми соглашениями с третьими сторонами, включая упомянутые в пунктах 26 и 28, должны оцениваться в соответствии с частью 12.2.

[32]Регламент (ЕС) 2016/679 Европейского Парламента и Совета от 27 апреля 2016 г. о защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных, и отмене Директивы 95/46/ЕС (Общие положения о защите данных, General Data Protection Regulation, GDPR)

[33]Финансовые организации должны обратиться к разделу V Руководства ЕВА по внутреннему управлению.

[34]См. статью 11 Директивы 2015/2366 (Вторая платежная Директива).

[35]См. Руководство ЕВА по управлению рисками в области ИКТ и безопасности (https://eba.europa.eu/-/eba-consults-on-guidelines-on-ict-and-security-risk-management) и основополагающие элементы G7 для управления киберрисками, связанными с третьими сторонами, в финансовом секторе (https://ec.europa.eu/info/publications/g7-fundamental-elements-cybersecurity-financial-sector_en).

34. Финансовые организации и платежные учреждения должны соответствовать всем требованиям Регламента (ЕС) 2016/679, в том числе в отношении аутсорсинга и соглашений с третьими лицами.

6 Надлежащие механизмы управления и аутсорсинг

35. Обязанности органов управления не должны делегироваться третьим сторонам. Финансовые организации и платежные учреждения всегда несут полную ответственность за соблюдение нормативных обязанностей, в том числе по надзору за аутсорсингом критических или существенных функций.

36. Орган управления всегда несет полную ответственность, по крайней мере, за:

    a. непрерывное соблюдение финансовыми организациями и платежными учреждениями регулятивных требований к ведению деятельности, в том числе отдельных требований налагаемых компетентными органами;

    b. внутреннюю организацию финансовой организации или платежного учреждения;

    c. выявление, оценку и урегулирование конфликтов интересов;

    d. разработку стратегий и внутренних правил финансовой организации или платежного учреждения (например, бизнес-модели, политики по уровню приемлемого риска, структуре управления рисками);

    e. надзор за текущим управлением финансовой организацией или платежным учреждением, включая управление рисками, связанными с аутсорсингом; и

    f. надзорную роль органа управления, включая надзор и контроль за принятием управленческих решений

37. Аутсорсинг не должен вести к снижению требований, предъявляемых к членам органа управления, директорам, ключевым должностным лицам и лицам, ответственным за управление платежным учреждением. Финансовые организации и платежные учреждения должны обладать надлежащей компетенцией, квалифицированными ресурсами в достаточном объеме для целей надлежащего управления соглашениями об аутсорсинге и надзора за ними.

38. Финансовые организации и платежные учреждения должны:

    a. распределить обязанности, связанные с документированием, администрированием и контролем за аутсорсингом;

b. выделить достаточные ресурсы для соблюдения всех правовых и нормативных требований, включая требования настоящего Руководства, а также для ведения контроля и мониторинга всех соглашений об аутсорсинге;

c. принимая во внимание часть 1 настоящего Руководства, создать подразделение по аутсорсингу или назначить ответственного сотрудника, который будет непосредственно подотчетен руководящему органу (например, ключевому должностному лицу, отвечающему за соответствующие контрольные функции). В сферу ответственности назначенного сотрудника или подразделения должно входить управление рисками, связанными с соглашениями об аутсорсинге, надзор за ними в рамках системы внутреннего контроля организации, а также контроль за документированием аутсорсинга. Небольшие финансовые организации или платежные учреждения, а также организации с более простой административной структурой должны, по крайней мере, распределить задачи и обязанности, связанные с администрированием и контролем за соглашениями об аутсорсинге. Эта функция может быть делегирована членам органа управления финансовой организации или платежного учреждения.

39. Финансовая организация или платежное учреждение должны оказывать фактические услуги, их деятельность не должна быть номинальной. В связи с этим, они обязаны:

a. непрерывно выполнять все условия выданного разрешения на ведения деятельности[36], включая эффективное выполнение органом управления своих обязанностей, изложенных в пункте 36 настоящего Руководства;

b. сохранять четкую и прозрачную организационную структуру, обеспечивающую соответствие всем юридическим и нормативным требованиям;

c. осуществлять надлежащий надзор и управлять рисками, возникающими в результате передачи на аутсорсинг операционной части внутреннего контроля

[36]См. нормативно-технические стандарты (regulatory technical standards (RTS)) в соответствии со статьей 8(2) Директивы 2013/36/ЕС об информации, которая должна предоставляться для выдачи кредитным организациям разрешения на ведение деятельности, и имплементирующие технические стандарты (implementing technical standards (ITS)) в соответствии со статьей 8(3) Директивы 2013/36/ЕС о стандартных формах, шаблонах и процедурах для предоставления информации, необходимой для выдачи кредитным организациям разрешения на ведение деятельности (https://eba.europa.eu/regulation-and-policy/other-topics/rts-and-its-on-the-authorisation-of-credit-institutions).

Платежным учреждениям также следует ознакомиться с Руководством ЕВА в рамках Второй платежной Директиве относительно информации, которая должна предоставляться для выдачи разрешения на ведение деятельности платежным учреждениям и учреждениям, эмитирующим электронные деньги, а также для регистрации провайдеров услуг по агрегации финансовой информации (https://eba.europa.eu/documents/10180/1904583/Final+Guidelines+on+Authorisations+of+Payment+Institutions+%28EBA-GL-2017-09%29.pdf).

(например, в случае аутсорсинга внутри группы компаний или в рамках институциональной системы защиты), управлять рисками, возникающими при аутсорсинге критических или существенных функций; и

d. располагать достаточными ресурсами для соблюдения пунктов (a)-(c).

40. При аутсорсинге финансовые организации и платежные учреждения должны, как минимум:

a. иметь возможность принимать и реализовывать решения, связанные с их деятельностью и с критическими и существенными функциями, в том числе теми, которые были переданы на аутсорсинг;

b. поддерживать упорядоченное ведение своей деятельности и предоставляемых банковских и платежных услуг;

c. должным образом идентифицировать, оценивать, регулировать и снижать риски, связанные с текущими и планируемыми соглашениями об аутсорсинге, включая риски, связанные с ИКТ и финансовыми технологиями (финтех);

d. предпринимать меры по обеспечению конфиденциальности данных и другой информации;

e. поддерживать надлежащий уровень информационного обмена с поставщиками услуг;

f. в отношении переданных на аутсорсинг критических или существенных функций, иметь возможность своевременно предпринять по крайней мере одно из следующих действий:

i. передать функцию альтернативным поставщикам услуг;

ii. реинтегрировать функцию, т.е. выполнять ее самостоятельно; или

iii. прекратить деятельности, зависящую от такой функции.

g. действовать в соответствии с Регламентом (ЕС) 2016/679, если поставщиками услуг обрабатываются персональные данные, вне зависимости от того, где территориально находятся поставщики услуг: в ЕС или в третьих странах.

7 Политика финансовой организации или платежного учреждения в отношении аутсорсинга

41. Орган управления финансовой организации или платежного учреждения[37], имеющего соглашения об аутсорсинге или планирующего заключить такие соглашения, должен

[37]См. Руководство ЕВА по мерам безопасности в отношении операционных рисков и угроз безопасности платежных сервисов в рамках Второй платежной Директивы: https://www.eba.europa.eu/regulation-and-

утвердить, регулярно пересматривать и обновлять политику в отношении аутсорсинга, а также, в зависимости от ситуации, следить за ее реализацией на индивидуальном уровне или уровне группы компаний. Политика финансовых организаций в отношении аутсорсинга должна соответствовать части 8 Руководства ЕВА по внутреннему управлению и, в частности, учитывать требования, изложенные в части 18 (новые продукты и существенные изменения)[38]. Платежные учреждения также могут привести свою политику в отношении аутсорсинга в соответствие с частями 8 и 18 Руководства ЕБА по внутреннему управлению.

42. Политика в отношении аутсорсинга должна охватывать основные этапы жизненного цикла аутсорсинговых соглашений, устанавливать принципы, определять обязанности и процессы, связанные с аутсорсингом. В частности, в политике должны быть определены по крайней мере следующие положения:

    a. обязанности органа управления в соответствии с пунктом 36, включая его участие, в случае необходимости, в принятии решений о передаче на аутсорсинг критических и существенных функций;

    b. привлечение соответствующих отделов организации, службы внутреннего контроля и других заинтересованных лиц при решении вопросов, связанных с аутсорсингом;

    c. разработку условий аутсорсинга, в том числе:

        i. утверждение бизнес-требований в отношении соглашений об аутсорсинге;

        ii. утверждение критериев, в том числе упомянутых в части 4, и разработка процесса выявления критических и существенных функций;

        iii. выявление, оценку и управление рисками в соответствии с частью 12.2;

        iv. комплексную проверку потенциальных поставщиков услуг, включая меры, установленные частью 12.3;

        v. описание процедуры выявления, оценки, урегулирования и снижения потенциальных рисков, связанных с конфликтом интересов, в соответствии с частью 8;

        vi. утверждение стратегии непрерывности ведения бизнеса в соответствии с частью 9;

policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2

[38] Часть 18 требует от поднадзорных организаций иметь отдельную политику по утверждению новых продуктов (NPAP, new product approval policy) на случай внедрения новых услуг/продуктов, выхода на новые рынки, существенных изменений в продуктах и используемых процессах – прим.пер.

vii. описание процесса утверждения новых соглашений об аутсорсинге;

d. процессы внедрения, мониторинга и управления соглашениями об аутсорсинге, включая:

i. текущую оценку деятельности поставщика услуг в соответствии с частью 14;

ii. процедуру уведомления и реагирования на изменения, внесенные в соглашение об аутсорсинге, или изменения, произошедшие у поставщика услуг (например, в его финансовом положении, организационной структуре, структуре собственности, субаутсорсинге);

iii. независимый контроль и аудит соблюдения правовых и нормативных требований, а также положений утвержденной политики;

iv. процедуры обновления текущих соглашений;

e. требования к документообороту и ведению учета в соответствии с требованиями части 11;

f. описание процесса расторжения соглашения об аутсорсинге и прекращения деятельности, включая план действий на случай, если оказание услуг по аутсорсингу критических и существенных функций будет осуществляться с перебоями или действие соглашения об аутсорсинге будет прекращено.

43. Организация, разрабатывая и утверждая политику в отношении аутсорсинга, должна учитывать следующее:

a. различия между соглашениями об аутсорсинге критических и существенных функций и иных соглашений об аутсорсинге;

b. имеет ли поставщик услуг, с которым заключается соглашение об аутсорсинге, разрешение на ведение деятельности, выданное компетентным органом;

c. заключено ли соглашение об аутсорсинге в рамках группы компаний, институциональной системы защиты (включая компании, полностью принадлежащие, индивидуально или коллективно, финансовым организациям в рамках институциональной системы защиты) или с внешним поставщиком услуг; и

d. находится ли поставщик услуг в государстве-члене ЕС или за его пределами.

44. Политикой организации в отношении соглашений об аутсорсинге критических или существенных фикций должны учитываться, в том числе в процессе принятия решений, следующие особенности организации (а также потенциальное влияние на них):

a. профиль рисков организации;

b. способность организации управлять рисками и осуществлять надзор за поставщиком услуг;

c. предпринимаемые организацией меры по обеспечению непрерывности бизнеса; и

d. особенности ведения деятельности.

8 Конфликт интересов

45. Финансовые организации, в соответствии с частью 11 раздела IV Руководства EBA по внутреннему управлению[39], и платежные учреждения должны выявлять, оценивать и урегулировать конфликты интересов в отношении соглашений об аутсорсинге.

46. Если аутсорсинг создает существенные конфликты интересов, в том числе между субъектами, входящими в одну группу компаний или институциональную систему защиты, финансовым организациям и платежным учреждениям необходимо принять надлежащие меры для урегулирования таких конфликтов.

47. Если функции переданы поставщику услуг, который является частью группы компаний, участником институциональной системы защиты либо он принадлежит финансовой организации, платежному учреждению, группе компаний или организациям, которые являются участниками институциональной системы защиты, то условия, включая финансовые, предоставления услуг аутсорсинга должны устанавливаться на дискриминационных условиях и как с независимой организацией. При установлении цены на аутсорсинг может приниматься во внимание, что поставщик оказывает одинаковые или схожие услуги нескольким компаниям группы или институциональной системы защиты, а потому цена может быть ниже. Тем не менее, следует обеспечить, чтобы бесперебойность оказания аутсорсинговых услуг не зависела от отношений внутри группы или проблем отдельных компаний группы.

9 Планы по обеспечению непрерывности деятельности

48. Финансовые организации, в соответствии с требованиями статьи 85(2) Директивы 2013/36/ЕС и раздела VI Руководства EBA по внутреннему управлению[40], и платежные учреждения должны разработать, поддерживать и периодически тестировать планы по обеспечению непрерывности деятельности в отношении переданных на аутсорсинг критических и существенных функций. Финансовые организации и платежные учреждения, функционирующие в рамках группы компаний

[39]Платежные учреждения также могут привести свою политику в соответствие с данным Руководством.

[40]Доступно по ссылке: https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised-

или институциональной системы защиты, могут руководствоваться централизованно разработанными планами по обеспечению непрерывности деятельности в отношении переданных на аутсорсинг функций.

49. Планы по обеспечению непрерывности деятельности должны учитывать ситуации, когда качество предоставления переданной на аутсорсинг критической или существенной функции опустится до неприемлемого уровня, либо при ее осуществлении произойдет сбой. Такие стратегии также должны учитывать потенциальные последствия неплатежеспособности поставщиков услуг, или другие сбои на стороне третьих лиц, а также, где это уместно, политические риски, находящиеся в юрисдикции поставщика услуг.

10 Внутренний аудит

50. В соответствии с риск-ориентированным подходом, служба внутреннего аудита[41] должна проводить независимую проверку аутсорсинговой деятельности. Также должен проводиться аудит[42] соглашений об аутсорсинге критических и существенных функций.

51. В отношении процесса аутсорсинга служба внутреннего аудита должна по крайней мере удостовериться, что:

    a. требования, предъявляемые к соглашениям об аутсорсинге, включая принятую в этой области политику, внедрены корректно и эффективно используются, а также соответствуют действующему законодательству, стратегии управления рисками и принятым органами управления решениям;

    b. критичность и существенность функций оцениваются адекватно, качественно и эффективно;

    c. риски, связанные с соглашениями об аутсорсинге, оцениваются адекватно, качественно и эффективно, а также соответствуют стратегии управления рисками;

    d. органы управления надлежащим образом вовлечены в процесс; и

[41]По вопросам обязанностей службы внутреннего аудита, финансовым организациям следует обратиться к части 22 Руководства EBA по внутреннему управлению (https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised-), а платежным учреждениям – к принципу 5 Руководства EBA по выдаче разрешений на ведение деятельности платежным учреждениям (https://eba.europa.eu/documents/10180/1904583/Final+Guidelines+on+Authorisations+of+Payment+Institutions+%28EBA-GL-2017-09%29.pdf).

[42]См. Руководство EBA по процессу оценки количественных и качественных характеристик деятельности и рисков кредитных организаций: 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

e. осуществляется надлежащий мониторинг и управление соглашениями об аутсорсинге.

11 Требования к документообороту

52. В рамках принятой стратегии управления рисками финансовые организации и платежные учреждения должны вести и своевременно обновлять реестр всех соглашений об аутсорсинге, заключенных самой организацией, и, где применимо, на субконсолидированном или консолидированном уровнях, как указано в части 2, а также должны надлежащим образом документировать все текущие соглашения об аутсорсинге, разделяя соглашения об аутсорсинге критических и существенных функций и иные соглашения об аутсорсинге. Принимая во внимание национальное законодательство, финансовые организации должны вести реестр расторгнутых соглашений об аутсорсинге и хранить соответствующие документы в течение определенного законом периода времени.

53. Принимая во внимание раздел I настоящего Руководства и условия, изложенные в пункте 23(d), финансовые организации и платежные учреждения, входящие в группу компаний, организации, постоянно аффилированные с центральным органом, или учреждения, которые являются участниками одной институциональной системы защиты, могут вести реестр централизованно.

54. В реестре по всем текущим соглашениям об аутсорсинге должна содержаться следующая информация:

a. номер соглашения об аутсорсинге;

b. дата начала действия соглашения и, если применимо, дата его продления, дата окончания действия соглашения и/или период времени, в течение которого поставщик услуг, финансовая организация или платежное учреждение должны сообщить об изменении статуса соглашения;

c. краткое описание функции, переданной на аутсорсинг, включая переданные на аутсорсинг данные, а также информация о том, были ли переданы персональные данные (например, путем указания "да" или "нет" в отдельной строке) и обрабатывает ли такие данные поставщик услуг;

d. категория, к которой относится функция, и присвоенная финансовой организацией или платежным учреждением, согласно пункту (c) (например, информационные технологии (IT), функция контроля) для целей классификации соглашений об аутсорсинге;

e. наименование поставщика услуг, регистрационный номер юридического лица, идентификатор юридического лица (LEI) (при наличии), юридический адрес и

другие контактные данные, а также наименование его головной компании (при наличии);

f. страна или страны, в которых будет оказываться услуга, включая местоположение (т.е. страна или регион), где будут храниться и/или обрабатываться данные;

g. считается ли (да/нет) переданная на аутсорсинг функция критической или существенной, включая краткое описание причин присвоения функции такого статуса;

h. в случае соглашения об аутсорсинге с поставщиком облачных услуг, информация об облачной инфраструктуре, т.е. является ли сервис публичным, частным, гибридным или общественным, а также информация о характере передаваемых данных и стране или регионе их хранении;

i. дата последней оценки критичности или существенности функции, переданной на аутсорсинг.

55. Если соглашение об аутсорсинге включает передачу критических или существенных функций, то реестр должен включать следующую дополнительную информацию:

a. перечень финансовых организаций, платежных учреждений и других компаний, принадлежащих одной группе или институциональной системе защиты, на которые распространяется соглашение об аутсорсинге;

b. является ли поставщик услуг или субподрядчик частью группы компаний или участником институциональной системы защиты либо принадлежит финансовым организациям или платежным учреждениям, входящим в группу компаний, участникам институциональной системы защиты;

c. дата последней оценки риска и краткое изложение основных результатов;

d. физическое лицо или исполнительный орган финансовой организации или платежного учреждения, утвердившее соглашение об аутсорсинге;

e. по праву какой страны заключено соглашение об аутсорсинге;

f. даты последних и запланированных аудитов, если применимо;

g. где применимо, названия всех субподрядчиков, которым передаются на субаутсорсинг значимые части критической или существенной функции, включая информацию о стране, в которой зарегистрированы субподрядчики, где будет выполняться услуга и, если применимо, о стране или регионе, где будут храниться данные;

h. результат оценки возможности замены поставщика услуг с присвоением категории «просто», «трудно», «невозможно», возможности реинтеграции

критической или существенной функции обратно в финансовую организацию или платежное учреждение, либо описание последствий прекращения осуществление критической или существенной функции;

i. перечень альтернативных поставщиков услуг в соответствии с пунктом (h);

j. влияет ли переданная на аутсорсинг критическая или существенная функция на бизнес-процессы, которые должны выполняться в четкие временные сроки;

k. предполагаемые годовые бюджетные расходы.

56. Финансовые организации и платежные учреждения должны по запросу компетентного органа предоставить ему либо полный реестр текущих соглашений об аутсорсинге[43], либо его отдельные разделы, например, информацию обо всех соглашениях об аутсорсинге, подпадающих под одну из категорий, упомянутых в подпункте (d) пункта 54 настоящего Руководства (к примеру, ИТ-аутсорсинг). Финансовые организации и платежные учреждения должны предоставлять эту информацию в машиночитаемом формате (например, в широко используемом формате базы данных, значения через запятую).

57. Финансовые организации и платежные учреждения должны по запросу компетентного органа предоставить ему всю необходимую информацию для целей эффективного надзора, включая, при необходимости, копии соглашений об аутсорсинге.

58. С учетом требований статьи 19(6) Директивы (ЕС) 2015/2366[44], финансовые организации и платежные учреждения должны надлежащим образом своевременно информировать компетентные органы о планируемом аутсорсинге критических или существенных функций и/или о случаях, когда функция, переданная на аутсорсинг, изменила статус на критическую или существенную и предоставить, как минимум, информацию, указанную в пункте 54.

59. Финансовые организации и платежные учреждения[45] должны своевременно информировать компетентные органы о существенных изменениях и/или значимых событиях, касающихся соглашений об аутсорсинге, которые могут оказать

[43]См. также Руководство EBA по процессу оценки количественных и качественных характеристик деятельности и рисков кредитных организаций: https://eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2

[44]Статья 19(6) устанавливает ряд признаков «важных операционных функций». К ним относятся те, сбои в осуществлении которых поставить под угрозу соблюдение условий, по которым платежному институту выдано разрешение на деятельность, финансовую стабильность организации, стабильность оказания платежной услуги – прим.пер.

[45]См. Руководство EBA по составлению отчетов о крупных инцидентах, подпадающих под Вторую платежную Директиву: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-major-incidents-reporting-under-psd2

существенное влияние на непрерывность деятельности финансовой организации или платежного учреждения.

60. Финансовые организации и платежные учреждения должны надлежащим образом документировать сделанные в соответствии с разделом IV оценки, а также результаты текущего мониторинга (например, производительность поставщика услуг, качество предоставления услуг, соблюдение договорных и нормативных требований, текущая оценка рисков).

Раздел IV - Процесс передачи функций на аутсорсинг

12 Анализ, проводимый до заключения соглашения об аутсорсинге

61. Перед заключением соглашения об аутсорсинге, финансовые организации и платежные учреждения должны:

a. выявить, касается ли соглашение об аутсорсинге критической или существенной функции, как указано в разделе II;

b. оценить, соблюдены ли нормативные требования, изложенные в части 12.1;

c. определить и оценить соответствующие риски в соответствии с частью 12.2;

d. провести надлежащую проверку потенциального поставщика услуг в соответствии с частью 12.3;

e. выявить и оценить возможный конфликт интересов в связи с планируемым соглашением об аутсорсинге в соответствии с частью 8.

12.1 Надзорные требования, применяемые к аутсорсингу

62. Финансовые организации и платежные учреждения могут передать на аутсорсинг функции, связанные с банковской деятельностью[46] или платежными услугами, требующими авторизации или получения разрешения от уполномоченного компетентного органа государства-члена ЕС, поставщику услуг, расположенному в том же или другом государстве-члене ЕС, только при соблюдении одного из следующих условий:

a. поставщик услуг авторизован или зарегистрирован компетентным органом для осуществления такой банковской деятельности или оказания соответствующих платежных услуг; или

[46]См. статью 9 Директивы 2013/36/ЕС (Директива о капитале) в отношении запрета лицам или предприятиям, не являющимся кредитными учреждениями, осуществлять деятельность по приему депозитов или других средств, подлежащих возврату, у населения.

b. поставщику услуг иным образом разрешено осуществлять такую банковскую деятельность или оказывать соответствующие платежные услуги в соответствии с национальным законодательством.

63. Финансовые организации и платежные учреждения могут передать на аутсорсинг функции, связанные с осуществлением банковской деятельности или оказанием платежных услуг, выполнение которых требует получения разрешения или регистрации компетентным органом государства-члена ЕС, поставщику услуг, расположенному в третьей стране, только в том случае, если выполняются следующие условия:

a. поставщик услуг авторизован или зарегистрирован компетентным органом и имеет право осуществлять такую банковскою деятельность или оказывать платежные услуги в третьей стране, а также находится под надзором соответствующего компетентного органа в этой третьей стране (далее - "надзорный орган");

b. между компетентными органами, ответственными за надзор за финансовой организацией, и надзорными органами, ответственными за надзор за поставщиком услуг, заключено соглашение о сотрудничестве, например, в форме меморандума о взаимопонимании;

c. соглашением о сотрудничестве, упомянутым в пункте (b), должно гарантироваться, что компетентные органы могут по крайней мере:

i. получать по запросу информацию, необходимую для выполнения надзорных функций в соответствии с Директивой 2013/36/ЕС, Регламентом (ЕС) № 575/2013, Директивой (ЕС) 2015/2366 и Директивой 2009/110/ЕС;

ii. получать доступ к любым данным, документам, помещениям или персоналу в третьей стране для целей эффективного надзора;

iii. в кратчайшие сроки получать информацию от надзорного органа в третьей стране для расследования явных нарушений требований Директивы 2013/36/ЕС, Регламента (ЕС) № 575/2013, Директивы (ЕС) 2015/2366 и Директивы 2009/110/ЕС; и

iv. сотрудничать с надзорными органами в третьей стране по вопросам правоприменения в случае нарушения нормативных требований и национального законодательства в государстве-члене ЕС. Сотрудничество должно включать, но не ограничиваться получением в возможно кратчайшие сроки информации о потенциальных нарушениях текущего законодательства от надзорных органов третьей страны.

12.2 Оценка рисков при заключении соглашений об аутсорсинге

64. До заключения соглашения об аутсорсинге, финансовые организации и платежные учреждения должны оценить потенциальное влияние аутсорсинга на операционные риски, учесть полученные результаты оценки при принятии решения о том, следует ли передавать функцию на аутсорсинг поставщику услуг, а также предпринять шаги, чтобы избежать неоправданных дополнительных операционных рисков.

65. Оценка рисков должна включать, где это уместно, описание возможных вариантов реализации риска, включая критически опасные сценарии, связанные с операционными рисками. В рамках такого анализа финансовые организации и платежные учреждения должны оценить потенциальное воздействие сбоев или неудовлетворительного предоставления услуг, включая риски, вызванные процессами, системами, человеческим фактором или внешними событиями. Финансовые организации и платежные учреждения, применяя принцип пропорциональности, упомянутый в части 1, должны задокументировать проведенный анализ и его результаты, а также оценить, в какой степени соглашение об аутсорсинге повлияет на их операционные риски. В соответствии с разделом I, небольшие финансовые организации или платежные учреждения, а также организации с более простой административной структурой, могут использовать качественные подходы к оценке рисков, в то время как крупные или сложноорганизованные учреждения должны использовать более сложный подход, включая, где это возможно, использование внутренних и внешних данных о потерях при анализе вариантов наступления риска.

66. В рамках оценки рисков финансовые организации и платежные учреждения должны учитывать ожидаемые выгоды и затраты, связанные аутсорсингом, включая сравнение рисков, которые можно минимизировать или которыми можно качественнее управлять, с любыми рисками, которые могут возникнуть в результате подписания соглашения об аутсорсинге, учитывая, как минимум:

    a. риски концентрации, в том числе возникающие в результате:

        i. аутсорсинга функций поставщику услуг, которому трудно найти замену; и

        ii. подписания нескольких соглашений об аутсорсинге с одним и тем же поставщиком услуг или тесно связанными поставщиками услуг;

    b. совокупные риски, возникающие в результате передачи нескольких функций на аутсорсинг в рамках финансовой организации или платежного учреждения, и, в случае группы компаний или институциональной системы защиты, совокупные риски, возникающие на консолидированной основе или в рамках системы защиты;

c. в случае значимых финансовых организаций, риск вынужденной поддержки, т.е. риск, который может возникнуть при необходимости оказывать финансовую поддержку поставщику услуг в случае его банкротства или тяжелого финансового положения, либо необходимости брать на себя операционное управление поставщиком услуг; и

d. меры по управлению и минимизации рисков, принятые финансовой организацией, платежным учреждением и поставщиком услуг.

67. Если соглашением об аутсорсинге предусмотрена возможность передачи критических или существенных функций на субаутсорсинг, финансовые организации и платежные учреждения должны учитывать:

a. риски, связанные с субаутсорсингом, включая дополнительные риски, которые могут возникнуть, если субподрядчик находится в третьей стране или стране, отличной от страны нахождения поставщика услуг;

b. риски, связанные с тем, что длинные и сложные цепочки субаутсорсинга снижают способность финансовых организаций или платежных учреждений осуществлять надзор за переданными на аутсорсинг критическими или важными функциями, а также влияют на эффективность контроля со стороны компетентных органов.

68. При проведении оценки рисков перед заключением соглашения об аутсорсинге и в процессе текущего мониторинга деятельности поставщика услуг финансовые организации и платежные учреждения должны как минимум:

a. определить и классифицировать соответствующие функции, а также связанные с ними данные и системы, с точки зрения их чувствительности и предъявляемых требований к безопасности;

b. провести тщательный риск-ориентированный анализ функций и связанных с ними данных и систем, которые рассматриваются для передачи на аутсорсинг либо уже переданы на аутсорсинг, и минимизировать потенциальные риски, в частности операционные риски, включая юридические, риски в области ИКТ, комплаенса и репутационные риски, а также риски, связанные с ограничением надзора в странах, где переданные на аутсорсинг услуги предоставляются или могут предоставляться в будущем, и где данные хранятся или могут храниться в будущем;

c. учесть местонахождение поставщика услуг (в ЕС или за его пределами);

d. учесть политическую ситуацию, в т.ч. стабильность и безопасность в рассматриваемых юрисдикциях, включая:

i. действующее законодательство, в т.ч. законы о защите данных;

ii. положения, касающиеся правоохранительной деятельности; и

iii. законодательство о банкротстве, которое будет применяться в случае банкротства поставщика услуг, а также любые ограничения, которые могут возникнуть в случае необходимости срочного восстановления данных финансовой организации или платежного учреждения;

e. определить надлежащий уровень защиты конфиденциальности данных, непрерывности деятельности, передаваемой на аутсорсинг, а также целостности и отслеживаемости данных и систем в контексте предполагаемого аутсорсинга. Финансовым организациям и платежным учреждениям следует также утвердить конкретные меры, если применимо, в отношении хранимых, передаваемых данных и данных, находящихся в оперативном доступе, например, использовать технологии шифрования в сочетании с соответствующей архитектурой управления ключами шифрования;

f. определить, является ли поставщик услуг дочерним или головным предприятием организации, включен ли в сферу консолидации бухгалтерского учета или является членом или собственностью организации-участницы институциональной системы защиты, а также определить, в какой степени организация контролирует поставщика услуг или имеет возможность влиять на его действия в соответствии с частью 2.

12.3 Надлежащая проверка

69. До заключения соглашения об аутсорсинге и оценки операционных рисков, связанных с подлежащей передаче на аутсорсинг функцией, финансовые организации и платежные учреждения в процессе оценки и выбора поставщика услуг должны убедиться в его репутации и надежности.

70. В отношении критических и существенных функций, финансовые организации и платежные учреждения должны убедиться, что поставщик услуг обладает требуемой деловой репутацией, надлежащими и достаточными навыками, экспертизой, потенциалом, ресурсами (например, людскими, ИТ, финансовыми), надлежащей организационной структурой и, если применимо, требуемыми регистрациями и разрешениями на ведение деятельности, выданными регулирующими органами, для целей надежного и профессионального выполнения критической или существенной функции в течение всего срока действия соглашения.

71. Финансовым организациям и платежным учреждениям следует при проведении надлежащей проверки потенциального поставщика услуг учитывать следующие дополнительные факторы (но не ограничиваться ими):

a. бизнес-модель поставщика услуг, специфика деятельности, масштаб, сложность, финансовое положение, организационная структура и групповая структура;

b. долгосрочные отношения с поставщиками услуг, которые уже прошли оценку и предоставляют услуги финансовой организации или платежному учреждению;

c. является ли поставщик услуг головным предприятием или дочерней компанией финансовой организации или платежного учреждения, включен ли в сферу консолидации бухгалтерского учета, является ли членом или собственностью организаций-участниц институциональной системы защиты, к которой принадлежит финансовая организация или платежное учреждение;

d. находится ли поставщик услуг под надзором компетентных органов.

72. В тех случаях, когда аутсорсинг предполагает обработку персональных или конфиденциальных данных, финансовые организации и платежные учреждения должны убедиться в том, что поставщик услуг использует соответствующие технические и организационные инструменты для защиты данных.

73. Финансовые организации и платежные учреждения должны обеспечить соответствие поставщиков услуг их внутренним ценностями и кодексу поведения. В частности, в отношении поставщиков услуг, расположенных в третьих странах, и, если применимо, их субподрядчиков, финансовые организации и платежные учреждения должны убедиться в том, что поставщик услуг действует этическим и социально ответственным образом и придерживается международных стандартов в области прав человека (например, Европейской конвенции по правам человека), охраны окружающей среды и условий труда, в т.ч. соблюдает запрет на использование детского труда.

13 Заключение соглашения об аутсорсинге

74. В письменном соглашении об аутсорсинге должны быть распределены и прописаны права и обязанности финансовой организации, платежного учреждения и поставщика услуг.

75. Соглашении об аутсорсинге критических или существенных функций должно, как минимум, включать:

a. описание функции, передаваемой на аутсорсинг;

b. дату начала и дату окончания соглашения, где применимо, а также период времени, в течение которого поставщик услуг, финансовая организация или платежное учреждение должны сообщить об изменении статуса соглашения;

c. применимое законодательство;

d. финансовые обязательства сторон;

e. разрешен ли субаутсорсинг критической или существенной функции или ее значимых частей; и, если да, то условия, указанные в части 13.1, которые распространяются на субаутсорсинг;

f. местоположение (т.е. регионы или страны), где будет предоставляться критическая или существенная функция и/или где будут храниться и обрабатываться данные, включая возможные местоположения их хранения, а также предъявляемые требования, включая требование уведомлять финансовую организацию или платежное учреждение о планируемой смене местоположения;

g. если применимо, положения, касающиеся доступности, целостности, конфиденциальности и сохранности данных, как указано в части 13.2;

h. право финансовой организации или платежного учреждения осуществлять текущий мониторинг деятельности поставщика услуг;

i. уровень качества предоставления услуг, включая точные количественные и качественные целевые показатели, для целей осуществления текущего мониторинга и, при необходимости, принятия своевременных корректирующих действий, если уровень качества предоставления услуг ниже прописанного в соглашении;

j. обязательство поставщика услуг отчитываться перед финансовой организацией или платежным учреждением, уведомлять о любых изменениях, которые могут оказать значимое влияние на способность поставщика услуг эффективно выполнять критическую или существенную функцию в соответствии с согласованным уровнем качества предоставления услуг и применимым законодательством, а также по запросу предоставлять отчеты служб внутреннего аудита поставщика услуг;

k. должен ли поставщик услуг осуществлять обязательное страхование определенных рисков и, если применимо, то необходимый уровень такой страховой защиты;

l. требование к внедрению и тестированию планов действий на случай чрезвычайных ситуаций;

m. гарантия доступа к данным, принадлежащим финансовой организации или платежному учреждению, в случае прекращения деятельности или банкротства поставщика услуг;

n. обязательство поставщика услуг сотрудничать с компетентными органами, осуществляющими надзор за финансовыми организациями и платежными учреждениями, или введенными в них временными администрациями, в том числе с назначенными ими лицами;

o. для финансовых организаций - ссылка на полномочия национального органа по разрешению споров, особенно на статьи 68 и 71 Директивы 2014/59/EC (BRRD[47]), и, в частности, описание ‘существенных обязательств’ в смысле статьи 68 этой Директивы;

p. неограниченное право финансовых организаций, платежных учреждений и компетентных органов проверять поставщика услуг, в особенности, в отношении критических или существенных функции, переданных на аутсорсинг, как указано в части 13.3;

q. право расторжения соглашения, как указано в части 13.4.

13.1 Субаутсорсинг критических или существенных функций

76. В соглашении об аутсорсинге должно быть указано, допускается ли субаутсорсинг критических или важных функций или их значимых частей.

77. Если субаутсорсинг критических или важных функций допускается, финансовые организации и платежные учреждения должны определить, является ли часть функции, передаваемая на субаутсорсинг, критической или существенной сама по себе, и, если таковой является, сделать соответствующую запись в реестре.

78. Если субаутсорсинг критических или важных функций допускается, письменное соглашение об аутсорсинге должно содержать следующее:

a. перечень всех видов деятельности, которые запрещается передавать на субаутсорсинг;

b. условия, которые должны соблюдаться при субаутсорсинге;

c. пункт о том, что поставщик услуг обязан осуществлять надзор за теми услугами, которые он передает на субаутсорсинг, и гарантировать выполнение всех договорных обязательств между ним и финансовой организацией или платежным учреждением;

[47] Bank Recovery and Resolution Directive, Директива о восстановлении и санации банков – прим.пер.

d. требование о предварительном получении поставщиком услуг специального или общего письменного согласия от финансовой организации или платежного учреждения на передачу данных на субаутсорсинг[48];

e. положение об обязанности поставщика услуг информировать финансовую организацию или платежное учреждение о планируемом субаутсорсинге или его существенных изменениях, в частности, в тех случаях, когда это может повлиять на способность поставщика услуг выполнять свои обязанности по соглашению об аутсорсинге, в том числе, если планируются существенные изменения, касающиеся самих субподрядчиков или периода уведомления. В частности, период уведомления должен позволять финансовой организации или платежному учреждению как минимум провести оценку рисков предполагаемых изменений и, в случае необходимости, отказать в субаутсорсинге или планируемых изменениях до их вступления в силу;

f. право финансовой организации или платежного учреждения выступать против предполагаемого субаутсорсинга или его существенных изменений, либо условие, при котором поставщику услуг в этом случае необходимо получить явное одобрение со стороны финансовой организации или платежного учреждения на субаутсорсинг;

g. право финансовой организации или платежного учреждения расторгнуть соглашение в случае ненадлежащего субаутсорсинга, например, когда субаутсорсинг существенно увеличивает риски для финансовой организации или платежного учреждения, либо когда поставщик услуг передает функции на субаутсорсинг без предварительного уведомления финансовой организации или платежного учреждения.

79. Финансовые организации и платежные учреждения должны разрешать субаутсорсинг только в том случае, если субподрядчик обязуется:

a. соблюдать действующее законодательство, регулятивные требования и договорные обязательства; и

b. предоставлять финансовой организации, платежному учреждению и компетентному органу такие же права доступа и право на проведение аудита, что и те, которые предоставляются поставщиком услуг.

80. Финансовые организации и платежные учреждения должны убедиться, что поставщик услуг надлежащим образом осуществляет надзор за субподрядчиками в соответствии с политикой, определенной финансовой организацией или платежным учреждением. Если предполагаемый субаутсорсинг может в значительной степени негативно

[48]См. статью 28 Регламента (ЕС) 2016/679.

повлиять на аутсорсинг критической или существенной функции, либо повлечь существенное увеличение рисков, в том числе в тех случаях, когда не будут соблюдены условия, указанные в пункте 79, финансовая организация или платежное учреждение должно воспользоваться своим правом вето, если такое право имеется, и/или расторгнуть соглашение.

13.2 Безопасность данных и систем

81. Финансовые организации и платежные учреждения должны следить, чтобы поставщики услуг соблюдали соответствующие стандарты ИТ-безопасности, если это применимо.

82. Финансовые организации и платежные учреждения должны установить требования к безопасности данных и систем в рамках соглашения об аутсорсинге и проводить текущий мониторинг их соблюдения, если это применимо (например, в контексте использования облачных сервисов или другого аутсорсинга ИКТ).

83. В случае аутсорсинга функций поставщикам облачных услуг, а также других соглашений об аутсорсинге, включающих обработку или передачу личных или конфиденциальных данных, финансовым организациям и платежным учреждениям следует применять риск-ориентированный подход к тому, где территориально (т.е. страна или регион) будут храниться и обрабатываться данные, а также к вопросам информационной безопасности.

84. Соблюдая требования Регламента (ЕС) 2016/679[49], финансовые организации и платежные учреждения при передаче услуг на аутсорсинг (в частности, в третьи страны) должны учитывать различия в национальных законодательствах о защите данных. Соглашение об аутсорсинге должно включать положение об обязанности поставщика услуг защищать конфиденциальную, личную или иным образом чувствительную информацию и соблюдать законодательные требования о защите данных, которые применяются к финансовой организации или платежному учреждению (например, защита персональных данных и соблюдение банковской тайны, либо аналогичные нормативные обязательства в отношении конфиденциальности данных клиентов, если это применимо).

[49]Регламент № 2016/679 от 27.04.2016 о защите физических лиц в связи с обработкой их персональных данных и о свободном движении этих данных (отменяет Директиву 95/46/ЕС). Директива № 2016/679 лучше известна по своей аббревиатуре – GDPR – прим.пер.

13.3 Право на доступ, на информацию и на аудит

85. Финансовые организации и платежные учреждения должны прописать в соглашении об аутсорсинге право службы внутреннего аудита на анализ переданной на аутсорсинг функции, с учетом риск-ориентированного подхода.

86. Независимо от критичности или важности переданной на аутсорсинг функции, письменные соглашения об аутсорсинге между финансовыми организациями и поставщиками услуг должны учитывать полномочия компетентных органов по сбору информации и проведению необходимых расследований в соответствии со статьей 63(1)(a) Директивы 2014/59/ЕС и статьей 65(3) Директивы 2013/36/ЕС[50] в отношении поставщиков услуг, расположенных в государстве-члене ЕС, а также должны обеспечивать эти права в отношении поставщиков услуг, расположенных в третьих странах.

87. При аутсорсинге критических или существенных функций, письменным соглашением об аутсорсинге должна предусматриваться обязанность поставщика услуг предоставлять финансовым организациям, платежным учреждениям и компетентным органам, включая ведомствам, ответственным за санацию, а также любому другому лицу, назначенному самими организациями или компетентными органами, следующее:

    a. полный доступ ко всем коммерческим помещениям (например, головным офисам и операционным центрам), включая доступ ко всем устройствам, системам, сетям, информации и данным, используемым для предоставления функции, переданной на аутсорсинг, включая соответствующую финансовую информацию, информацию о персонале и внешних аудиторах поставщика услуг (‘право на доступ и право на информацию’); и

    b. неограниченные права на инспекцию и аудит, связанные с соглашением об аутсорсинге ("право на аудит"), позволяющие контролировать исполнение соглашения об аутсорсинге и обеспечивать соблюдение всех применимых нормативных и договорных требований.

88. При аутсорсинге функций, которые не являются критическими или существенными, финансовые организации и платежные учреждения должны, руководствуясь риск-ориентированным подходом, обеспечить для себя необходимый уровень прав на доступ и на аудит, как указано в пунктах 87(a) и (b) и части 13.3, учитывая характер передаваемой на аутсорсинг функции, операционные и репутационные риски, ее масштабируемость, потенциальное влияние на непрерывность деятельности и срок

[50] Указанные нормы относятся к праву компетентных органов запрашивать и получать любую релевантную информацию от любых лиц – прим.пер.

действия соглашения. Следует также принять во внимание, что со временем функция может поменять статус на критическую или существенную.

89. Финансовые организации и платежные учреждения должны убедиться, что соглашение об аутсорсинге или любое другое договорное соглашение не препятствует и не ограничивает эффективную реализацию права на доступ и на аудит ими самими, компетентными органами или третьими сторонами, назначенными ими для реализации этих прав.

90. Финансовые организации и платежные учреждения должны реализовывать свои права на доступ и на аудит, определять частоту аудита, а также областей, подлежащих аудиту, на основе риск-ориентированного подхода, и придерживаться соответствующих общепринятых национальных и международных стандартов аудита[51].

91. Финансовые организации и платежные учреждения, принимая во внимание свою конечную ответственность в отношении соглашений об аутсорсинге, могут использовать:

    a. совместные аудиты, организованные вместе с другими клиентами того же поставщика услуг и выполняемые совместно, либо назначенной ими третьей стороной, с целью более эффективного использования аудиторских ресурсов и снижения организационной нагрузки как на клиентов, так и на поставщика услуг;

    b. предоставленные поставщиком услуг сертификаты, выданные третьими сторонами, и отчеты об аудите, проведенном третьей стороной, либо о внутреннем аудите.

92. При передаче критической или существенной функции на аутсорсинг, финансовые организации и платежные учреждения должны оценить, являются ли сертификаты и отчеты третьих сторон, упомянутые в пункте 91(b), адекватными и достаточными для соблюдения законодательства. Финансовым организациям и платежным учреждениям не следует полагаться исключительно на эти отчеты в течение долгого периода времени.

93. Финансовые организации и платежные учреждения должны использовать метод, упомянутый в пункте 91(b), только в том случае, если они:

    a. удовлетворены планом аудита для функции, переданной на аутсорсинг;

[51] Финансовым организациям следует обратиться к части 22 Руководства EBA по внутреннему управлению: https://eba.europa.eu/documents/10180/1972987/Final+Guidelines+on+Internal+Governance+%28EBA-GL-2017-11%29.pdf/eb859955-614a-4afb-bdcd-aaa664994889

b. уверены, что сертификаты или аудиторские отчеты охватывают все соответствующие системы (включая процессы, приложения, инфраструктуру, центры обработки данных и т.д.), ключевые средства контроля, определенные финансовой организацией или платежным учреждением, а также соответствуют нормативным требованиям;

c. тщательно проверяют содержание сертификатов или аудиторских отчетов, а также их актуальность;

d. убедились, что оценка ключевых систем и средств контроля будут включены в будущие аудиторские отчеты;

e. удовлетворены компетентностью стороны, осуществляющей сертификацию или аудит (например, в отношении ротации аудиторской компании, квалификации, опыта, осуществления повторных проверок приведенных в отчете данных);

f. убедились, что при выдаче сертификатов и проведении аудита были соблюдены широко признанные профессиональные стандарты, а также, что они включают в себя проверку операционной эффективности действующих ключевых средств контроля;

g. имеют право запрашивать расширение области охвата сертификатов или аудиторских отчетов на другие системы и средства контроля; количество и частота таких запросов должны быть разумными и законными с точки зрения управления рисками; и

h. сохраняют за собой право проводить индивидуальные аудиты по своему усмотрению в отношении критических или существенных функций, переданных на аутсорсинг.

94. В соответствии с Руководством EBA по оценке рисков в области ИКТ в рамках SREP, финансовым организациям необходимо, если применимо, иметь возможность проводить тестирование на предмет проникновения в систему безопасности для оценки эффективности внедренных процессов и мер по кибербезопасности и внутренней безопасности ИКТ[52]. Принимая во внимание раздел I, платежные учреждения также должны иметь внутренние механизмы контроля за ИКТ, включая контроль безопасности ИКТ и меры по минимизации соответствующих рисков.

95. Планируя выездную проверку, финансовые организации, платежные учреждения, компетентные органы, аудиторы или третьи стороны, действующие от имени финансовой организации, платежного учреждения или компетентных органов,

[52] См. Руководство EBA по рискам в области ИКТ: https://www.eba.europa.eu/documents/10180/1841624/Final+Guidelines+on+ICT+Risk+Assessment+under+SREP+%28EBA-GL-2017-05%29.pdf/ef88884a-2f04-48a1-8208-3b8c85b2f69a

должны в разумные сроки уведомить об этом поставщика услуг, за исключением случаев, когда это невозможно из-за чрезвычайной или кризисной ситуации, либо привело бы к неэффективности проведения аудита.

96. При проведении аудитов совместно с несколькими клиентами следует проявлять осмотрительность в целях минимизации рисков для другого клиента (например, влияние на качество обслуживания, доступ к данным, конфиденциальность).

97. В тех случаях, когда соглашение об аутсорсинге касается высокого уровня технической сложности, например, в случае аутсорсинга облачных услуг, финансовые организации или платежные учреждения должны убедиться, что аудитор – будь это его внутренние аудиторы, пул аудиторов или внешние аудиторы, действующие от его имени, – обладает надлежащими и релевантными навыками и знаниями для эффективного проведения соответствующих аудитов и/или оценок. То же самое относится к персоналу финансовой организации или платежного учреждения, проверяющему сторонние сертификаты или аудиторские отчеты, предоставленные поставщиками услуг.

13.4 Прекращение действия соглашения

98. Соглашение об аутсорсинге должно прямо предусматривать право финансовых организаций и платежных учреждений расторгнуть соглашение в соответствии с действующим законодательством, в том числе в следующих случаях:

    a. если поставщик услуг нарушает действующее законодательство, нормативные акты или положения соглашения;

    b. если выявлены факторы, способные повлиять на исполнение функции, переданной на аутсорсинг;

    c. если имеют место существенные изменения в порядке аутсорсинга или влияющие на самого поставщика услуг (например, в случае субаутсорсинга или смены субподрядчиков);

    d. если выявлено некачественное управление конфиденциальными, личными или иным образом чувствительными данными или информацией, либо нарушается их безопасность; и

    e. если такое предписание выдано компетентным органом, осуществляющим надзор за финансовой организацией или платежным учреждением, например, в случае, когда по причине заключения соглашения об аутсорсинге компетентный орган больше не имеет возможности надлежащим образом осуществлять надзор за финансовой организацией или платежным учреждением.

99. Соглашением об аутсорсинге должна быть предусмотрена возможность передачи функции другому поставщику услуг или обратно в финансовую организацию или платежное учреждение. Для этих целей соглашение об аутсорсинге должно содержать:

a. четко прописанные обязательства, накладываемые на текущего поставщика услуг при передаче функции другому поставщику услуг или обратно финансовой организации или платежному учреждению, включая обязательства по обработке данных;

b. для снижения риска сбоев необходимо установить переходный период, в течение которого поставщик услуг после прекращения действия соглашение об аутсорсинге должен продолжать осуществлять функцию, переданную на аутсорсинг; и

c. обязательство, по которому поставщик услуг, в случае прекращения действия соглашения об аутсорсинге, должен содействовать финансовой организации или платежному учреждению в процессе передачи функции.

14 Надзор за функциями, переданными на аутсорсинг

100. Финансовые организации и платежные учреждения должны осуществлять текущий риск-ориентированный мониторинг работы поставщиков услуг в отношении всех соглашений об аутсорсинге, с акцентом на аутсорсинг критических или существенных функций, включая мониторинг доступности, целостности и безопасности данных и информации. В тех случаях, когда риски, характер или масштаб функции, переданной на аутсорсинг, существенно изменились, финансовые организации и платежные учреждения должны провести новую оценку критичности или существенности этой функции в соответствии с частью 4.

101. Финансовые организации и платежные учреждения должны надлежащим образом, тщательно и профессионально контролировать и управлять соглашениями об аутсорсинге.

102. Финансовые организации и платежные учреждения должны регулярно проводить оценку рисков в соответствии с частью 12.2 и с определенной периодичностью отчитываться перед органом управления о рисках, выявленных в связи с передачей критических или существенных функций на аутсорсинг.

103. Финансовые организации и платежные учреждения должны отслеживать и управлять внутренними рисками концентрации, обусловленными соглашениями об аутсорсинге, с учетом требований части 12.2 настоящего Руководства.

104. Финансовые организации и платежные учреждения должны на протяжении действия соглашения об аутсорсинге гарантировать, что эти соглашения, с акцентом на критические или существенные функции, соответствуют стандартам эффективности и качества в соответствии с внутренней политикой организации. Для этих целей организация должна:

    a. получать соответствующие отчеты от поставщиков услуг;

    b. проводить оценку работы поставщиков услуг, используя такие инструменты, как ключевые показатели эффективности, ключевые контрольные показатели, отчеты о предоставлении услуг, самосертификация и сторонний анализ; и

    c. проводить анализ иной информации, полученной от поставщика услуг, включая отчеты о принимаемых мерах по обеспечению непрерывности деятельности и результатах тестирований.

105. В случае, если финансовая организация выявила недочеты при исполнении функции, переданной на аутсорсинг, она должна предпринять соответствующие меры. В частности, финансовые организации и платежные учреждения должны отслеживать любые признаки того, что поставщики услуг выполняют переданную на аутсорсинг критическую или существенную функцию неэффективно или нарушая текущее законодательство и нормативные требования. При выявлении недочетов финансовые организации и платежные учреждения должны предпринять соответствующие корректирующие меры. При необходимости, такие меры могут включать в себя немедленное расторжение соглашения об аутсорсинге.

15 Стратегия выхода из соглашения об аутсорсинге

106. При передаче на аутсорсинг критических или существенных функций финансовым организациям и платежным учреждениям необходимо разработать и задокументировать стратегию выхода из соглашения, которая соответствует их политике в отношении аутсорсинга и планам по обеспечению непрерывности деятельности[53]. В стратегии должны быть прописаны по крайней мере следующие возможные ситуации:

    a. прекращение действия соглашения об аутсорсинге;

    b. сбой на стороне поставщика услуг;

[53] Финансовые организации, в соответствии с требованиями статьи 85(2) Директивы 2013/36/ЕС и раздела VI Руководства ЕВА по внутреннему управлению, и платежные учреждения должны иметь соответствующий план по обеспечению непрерывности деятельности в отношении передачи на аутсорсинг критических или существенных функций.

c. ухудшение качества осуществляемой функции и фактические или потенциальные сбои в работе, вызванные ненадлежащим исполнением этой функции;

d. существенные риски, влияющие на надлежащее и непрерывное осуществление функции.

107. Выход финансовой организации или платежного учреждения из соглашения об аутсорсинге не должен влиять на непрерывность деятельности, соблюдение действующего законодательства и качество предоставления услуг клиентам. Для этих целей финансовой организации или платежному учреждению необходимо:

a. разработать, внедрить и задокументировать комплексную стратегию выхода из соглашений об аутсорсинге и, при необходимости, протестировать ее (например, путем проведения анализа потенциальных финансовых и ресурсных затрат, влияния выхода из соглашения на деятельность, а также анализа временных затрат на передачу услуг на аутсорсинг альтернативному поставщику); и

b. определить альтернативные решения и разработать переходный план, позволяющий финансовой организации или платежному учреждению забрать функции и данные, переданные на аутсорсинг, у поставщика услуг и передать их альтернативному поставщику или внедрить обратно в саму финансовую организацию или платежное учреждение, либо предпринять другие меры, которые обеспечат непрерывное предоставление критической или существенной функции. При этом следует принимать во внимание проблемы, которые могут возникнуть из-за территориального расположения данных, а также реализовать необходимые меры для обеспечения непрерывности деятельности на переходном этапе.

108. При разработке стратегий выхода из соглашения финансовые организации и платежные учреждения должны:

a. определить цели стратегии выхода;

b. провести анализ влияния на деятельность, в т.ч. проанализировать риски, связанные с переданными на аутсорсинг процессами, услугами или другими видами деятельности, определить людские, финансовые и временные ресурсы, которые потребуются для реализации плана выхода;

c. распределить роли, обязанности и ресурсы для реализации плана выхода и переходных мероприятий;

d. определить критерии успешности передачи функций и данных при выходе из соглашения об аутсорсинге; и

e. определить показатели, которые будут использоваться для мониторинга соглашения об аутсорсинге (как описано в части 14), включая показатели неприемлемого качества обслуживания, в результате чего соглашение об аутсорсинге должно быть расторгнуто.

Раздел V – Положения, адресованные компетентным органам

109. При разработке надлежащих методов надзора за соблюдением финансовыми организациями и платежными учреждениями условий выданного разрешения на ведение деятельности, компетентные органы должны определить, приводят ли соглашения об аутсорсинге к существенному изменению этих условий и нарушению соответствующих обязательств.

110. Компетентные органы должны удостовериться, что они могут эффективно осуществлять надзор за финансовыми организациями и платежными учреждениями, в т.ч. что финансовые организации или платежные учреждения учли в рамках своего соглашения об аутсорсинге обязанность поставщиков услуг предоставлять права аудита и доступа компетентному органу и организации в соответствии с частью 13.3.

111. Анализ рисков аутсорсинга должен проводиться финансовыми организациями как минимум с использование системы SREP или, в отношении платежных учреждений, в рамках других надзорных процессов, включая специальные запросы или инспекции на местах.

112. В дополнение к информации, зарегистрированной в реестре, согласно части 11, компетентные органы могут запрашивать у финансовых организаций и платежных учреждений дополнительную информацию, в частности, о критических или существенных соглашениях об аутсорсинге:

    a. подробный анализ рисков;

    b. есть ли у поставщика услуг стратегия по обеспечению непрерывности деятельности с учетом специфики услуг, переданных им на аутсорсинг финансовой организацией или платежным учреждением;

    c. стратегию выхода из соглашения об аутсорсинге, если соглашение расторгается одной из сторон или если возникают перебои в предоставлении услуг; и

    d. имеющиеся ресурсы и разработанные меры для надлежащего мониторинга переданной на аутсорсинг деятельности.

113. В дополнение к информации в соответствии с частью 11, компетентные органы могут потребовать от финансовых организаций и платежных учреждений предоставить

подробную информацию о любом соглашении об аутсорсинге, даже если соответствующая функция не считается критической или существенной.

114. Компетентные органы должны оценить, с учетом риск-ориентированного подхода, следующее:

    a. надлежащим ли образом финансовые организации и платежные учреждения управляют и осуществляют мониторинг соглашений об аутсорсинге, в частности, критических или существенных функций;

    b. располагают ли финансовые организации и платежные учреждения достаточными ресурсами для мониторинга соглашений об аутсорсинге и управления ими;

    c. выявляют и управляют ли финансовые организации и платежные учреждения всеми соответствующими рисками; и

    d. выявляют ли финансовые организации и платежные учреждения конфликты интересов, оценивают ли они их и надлежащим ли образом управляют ими в контексте соглашений об аутсорсинге, например, в случае внутригруппового аутсорсинга или аутсорсинга в рамках одной и той же институциональной системы защиты.

115. Компетентные органы должны следить, чтобы деятельность финансовых организаций и платежных учреждений ЕС/ЕЭЗ не была номинальной, включая ситуации, когда учреждения используют взаимные транзакции или внутригрупповые транзакции для передачи части рыночного и кредитного риска субъекту, не находящемуся в зоне ЕС/ЕЭЗ. Также следует убедиться, что у финансовых организаций и платежных учреждений внедрены системы выявления и управления риска и выстроена соответствующая система корпоративного управления.

116. При проведении оценки компетентные органы должны учитывать все сопутствующие риски, в частности:[54]

    a. операционные риски[55], связанные с соглашением об аутсорсинге;

    b. репутационные риски;

[54]Финансовым организациям, подпадающим под действие Директивы 2013/36/ЕС, следует обратиться к Руководству ЕВА по SREP: https://eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2

[55]См. Руководство ЕВА по рискам в области ИКТ: https://www.eba.europa.eu/documents/10180/1841624/Final+Guidelines+on+ICT+Risk+Assessment+under+SREP+%28EBA-GL-2017-05%29.pdf/ef88884a-2f04-48a1-8208-3b8c85b2f69a

c. риск вынужденной поддержки, при наступлении которого значимая организация будет вынуждена оказать существенную помощь поставщику услуг;

d. риски концентрации внутри организации, в том числе на консолидированной основе, вызванные множественными соглашениями об аутсорсинге с одним поставщиком услуг или тесно связанными поставщиками услуг, либо несколькими соглашениями об аутсорсинге в рамках одной и той же сферы деятельности;

e. риски концентрации на уровне сектора, например, когда несколько финансовых организаций или платежных учреждений используют одного поставщика услуг или небольшую группу поставщиков услуг;

f. степень, в которой финансовая организация или платежное учреждение контролирует поставщика услуг или имеет возможность влиять на его действия, а также потенциальное снижение рисков в результате более высокого уровня контроля и в тех случаях, когда поставщик услуг включен в консолидированный надзор группы; и

g. риски конфликтов интересов между финансовыми организациями и поставщиками услуг.

117. При выявлении рисков концентрации компетентным органам следует отслеживать развитие таких рисков и оценивать как их потенциальное воздействие на другие финансовые организации и платежные учреждения, так и на стабильность финансового рынка в целом; компетентным органам следует, при необходимости, информировать ведомство, ответственное за санацию банков, о новых потенциально критических функциях[56], выявленных в ходе этой оценки.

118. Если компетентные органы приходят к заключению, что финансовая организация или платежное учреждение больше не имеет надежных механизмов управления или не соответствует регулятивным требованиям, им следует предпринять такие меры, как ограничение перечня функций, передаваемых на аутсорсинг, или требование отказаться от одного или нескольких видов аутсорсинга. В частности, учитывая обязанность финансовой организации или платежного учреждения поддерживать непрерывность деятельности, компетентные органы могут потребовать расторжения соглашений об аутсорсинге, если надлежащий надзор и соблюдение действующего законодательства не могут быть обеспечены другими мерами.

119. Компетентные органы должны иметь все инструменты для осуществления эффективного надзора, в частности, когда финансовая организация или платежное

[56]Как определено в статье 2(1)(35) Директивы 2014/59/EC (BRRD).

учреждение передает критические или существенные функции на аутсорсинг организации, находящейся за пределами ЕС/ЕЭЗ.

Данная публикация предназначена только для ознакомления. Представленный перевод является неофициальным и не имеет юридической силы.

Ассоциация «АЭД» не несет ответственности за прямые или косвенные убытки, которые могут понести третьи лица, руководствуясь содержанием настоящей публикации.

Оригинал Руководства на английском языке доступен по адресу https://clck.ru/343NnX.

Предложения и комментарии к тексту данного документа Вы можете направить по адресу npaed@npaed.ru.