# **Оценка степени соответствия требованиям GDPR**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № п/п | Требование | Основание требования | Заключение о степени выполнения требования | Степень выполнения**[1]** | Рекомендации |
| **1.** | Требования, неисполнение или нарушение которых ведет к штрафам в размере до 20 млн евро или 4% общегодового мирового оборота компании | | | | |
|  | Соблюдение правомерности, справедливости и открытости обработки персональных данных (lawfulness, fairness and transparency) | 1 (a) article 5 GDPR | На русской версии сайта<https://www.yclients.com/> размещена Политика Конфиденциальности, но на английской и венгерской версиях сайта отсутствует ссылка на Privacy Policy. При этом на венгерской версии сайта присутствует оговорка об об обработке cookie.  В мобильном приложении Yclients отсутствует ссылка ан Privacy Policy в формах регистрации и авторизации.  На странице записи к Лицензиатам отсутствует ссылка на Privacy Policy Контроллера. | ВЧ | 1. Рекомендуется разработать документ Privacy Policy на трех языках (английский, русский и венгерский). Утверждать документ необходимо приказом Генерального директора Контроллера. Упомянутые в дальнейшем документы также будет необходимо утверждать приказом Генерального директора Контроллера.  2. Рекомендуется разместить ссылки на соответствующие языковые версии Privacy Policy на английской и венгерской версиях сайта<https://www.yclients.com/>, страницах записи к Лицензиатам и в мобильном приложении Yclients.  3. Рекомендуется добавить в Privacy Policy информацию об обработке cookie, т.к. они согласно GDPR также являются персональными данными. |
| 1.2. | Соблюдение сбора и обработки персональных данных в конкретных, ясных и законных целях | 1 (b) article 5 GDPR | На момент проведения обследования у Контроллера выявлено, что в Политике конфиденциальности описаны цели обработки персональных данных. | ВЧ | 1. Рекомендуется добавить цели обработки персональных данных в разрабатываемую Privacy Policy из Политики конфиденциальности. |
| 1.3. | Соблюдение условий по обработке достоверных и соответствующих целям обработки персональных данных (data minimisation) | 1 (c) article 5 GDPR | Контроллером не проводились мероприятия, направленные на минимизацию состава обрабатываемых персональных данных. | НВ | 1. Рекомендуется пересмотреть все имеющиеся процессы обработки персональных данных на предмет возможной минимизации обрабатываемых в них персональных данных и внедрить соответствующий регулярный процесс. |
| 1.4. | Соблюдение точности обрабатываемых персональных данных (accuracy) | 1 (d) article 5 GDPR | У Контроллера не определены меры, направленные на выявление неточных персональных данных для всех категорий субъектов данных. | НВ | 1. Рекомендуется зарегистрированным работникам Лицензиата показывать в личном кабинете раз в 6 месяцев уведомление о необходимости уточнить свои персональные данные, если они изменились.  2. Рекомендуется подписчикам на новостную рассылку направлять письмо с необходимостью уточнить свои персональные данные спустя 3 месяца после даты последнего непрочитанного письма. Если ответа не поступает, то блокировать и удалять таких пользователей с уведомлением о факте удаления. |
| 1.5. | Соблюдение сроков хранения персональных данных (storage limitation) | 1 (e) article 5 GDPR | В Политике конфиденциальности Контроллера установлены сроки хранения персональных данных.  Контроллер не производит контроль исполнения сроков хранения персональных данных. | ВЧ | 1. Рекомендуется перенести сроки хранения персональных данных из Политики конфиденциальности в разрабатываемую Privacy Policy.  2. Рекомендуется внедрить процесс контроля за сроками хранения персональных данных, чтобы они не нарушались. |
| 1.6. | Соблюдение целостности и конфиденциальности персональных данных при их обработке (integrity and confidentiality) | 1 (f) article 5 GDPR | Контроллер не осуществляет меры направленные на конфиденциальности и целостности персональных данных.  . | НВ | 1. Для информационной системы Yclients  рекомендуется провести Data Protection Impact Assessment (DPIA) и на этом основании определить меры (контроли), направленные на соблюдение целостности и конфиденциальности обрабатываемых персональных данных. |
| 1.7. | Подтверждение соблюдения принципов обработки персональных данных (accountability) | 2 article 5 GDPR | В Privacy Policy Контроллера не отображены сведения о выполнении им принципов обработки персональных данных. | НВ | 1. Рекомендуется отобразить в документе Privacy Policy и о принципах обработки персональных данных из ст.5 GDPR и их выполнении Контроллером.  2. Рекомендуется разработать веб-страницу с отображением информации о том, как организация выполняет принципы и требования GDPR (пример,<https://www.salesforce.com/gdpr/overview/>). |
| 1.8. | Наличие правомерных условий для обработки персональных данных | article 6 GDPR | Контроллер имеет правовые основания для обработки всех персональных данных. | ВП |  |
| 1.9. | Наличие подтверждений получения согласий на обработку персональных данных | 1 article 7 GDPR | В необходимых случаях Контроллер собирает согласия на обработку персональных данных посетителей сайтов и согласия на получение рассылок. Контроллером не собираются факты о получении таких согласий. | НВ | 1. Рекомендуется вынести из Правил пользования сервиса согласие на обработку персональных данных и сделать его отдельным чекбоксом с ссылкой на Privacy Policy под формой записи. Логи проставления галочки в чек-боксе необходимо сохранять в течение 3х лет.  2. Рекомендуется сохранять логи согласия посетителей сайта на обработку их cookie. Рекомендуется использовать специализированные сервисы, пример,<https://www.cookiebot.com/en/>. |
| 1.10. | Исполнение условия по получению письменного согласия на обработку персональных данных | 2 article 7 GDPR | При обработке персональных данных у Контроллера отсутствуют случаи, для которых необходима обработка с получением письменного согласия на обработку персональных данных. | ВНТ |  |
| 1.11. | Исполнение условия по простому отзыву согласия на обработку персональных данных | 3 article 7 GDPR | Отсутствуют инструкции по простому отзыву согласий на обработку cookie-файлов и сведениях о поведении пользователей на венгерской версии сайта Контроллера. В рассылаемых письмах Контролера есть простой отзыв согласия путем перехода по ссылке. | ВЧ | Рекомендуется использовать на венгерской версии сайта Контроллера использовать сервис<https://www.cookiebot.com/en/>, который позволяет пользователям управлять своими согласиями на обработку, в т.ч. удалять их (равноценно отзыву согласия). |
| 1.12. | Исполнение условия предоставления согласия на обработку персональных данных по доброй воле | 4 article 7 GDPR | В п.2.4. Правил использования сервиса (<https://www.yclients.com/info/rules>) вшито согласие на обработку персональных данных в целях осуществления рекламы. Принимая вышеуказанные правила пользователь по умолчанию дает согласие, что является нарушением и согласием данным не по доброй воле. | НВ | 1. Рекомендуется вынести из Правил пользования сервиса согласие на обработку персональных данных и сделать его отдельным чекбоксом с ссылкой на Privacy Policy под формой записи. |
| 1.13. | Выполнение условий обработки чувствительных категорий персональных данных | article 9 GDPR | Контроллером не обрабатываются чувствительные категории персональных данных | ВНТ |  |
| 1.14. | Предоставление информации субъекту данных в установленные сроки | article 12 GDPR | У контроллера не регламентированы публично обязательства об исполнении прав субъектов данных по GDPR. | НВ | 1. Рекомендуется разработать документ Subject Access Requests General Guidance, описывающий реализацию прав физических лиц в течение 30 дней с момента получения запроса от субъекта данных с возможностью продления сроков обработки запроса до 90 дней и описать реализацию прав субъектов данных по GDPR.  2. Рекомендуется добавить в разрабатываемый документ Privacy Policy информацию о правах субъектов данных, которые они могут реализовать, сроках реагирования на запросы, возможность запроса дополнительной информации для идентификации человека, предупреждение о том, что если запросы от субъекта данных будут являться явно не обоснованными или чрезмерными, то Контроллер имеет право взымать разумную плату за реагирование на запрос или отказаться действовать с таким запросом. |
| 1.15. | Предоставление информации при получении персональных данных от субъекта данных (Privacy Notice) | article 13 GDPR | В публичных документах Контроллера отображена не вся информация, которая должна быть в Privacy Notice. | НВ | 1. Рекомендуется добавить в разрабатываемую Privacy Policy следующую информацию:  - указать цели обработки персональных данных из Политики конфиденциальности  - добавить информацию о третьих лицах, которым передаются персональные данные и поручаются на обработку;  - добавить информацию о законных основаниях обработки персональных данных;  - добавить информацию об имеющихся у физических лиц правах и возможностях их реализации;  - добавить информацию об отсутствии или наличии автоматического принятия решений на основании обработки персональных данных;  - добавить контактную информацию о представителе Контроллера на территории ЕС;  - добавить более точные сведения о сроках, в течение которых будут храниться персональные данные или, если это не представляется возможным, критерии для определения такого срока. |
| 1.16. | Предоставление информации при получении персональных данных не от субъекта данных | article 14 GDPR | Контроллер получает персональные данные только напрямую от субъектов данных, или в качестве процессора от клиентов. | ВНТ |  |
| 1.17. | Выполнение прав субъектов персональных данных на доступ к персональным данным | article 15 GDPR | В локальных документах Контроллера и документе Privacy Policy не отображено право субъектов данных на доступ к персональным данным и не регламентированы шаги по доступу субъектов данных к своим персональным данным. | ВЧ | 1. Рекомендуется в документах Privacy Policy и Subject Access Requests General Guidance прописать возможность реализации права субъектов данных на доступ к своим персональным данным, а также:  - о цели обработки;  - о соответствующих категориях обрабатываемых персональных данных;  - о получателях или категории получателей, которым персональные данные были либо будут раскрыты, в том числе, о получателях в третьих странах или о международных организациях;  - о предполагаемом сроке, когда это возможно, в течение которого будут храниться персональные данные, или, если это невозможно, о критериях, используемых для определения указанного срока;  - о наличии права требовать от Контроллера исправления или удаления соответствующих персональных данных, или ограничения их обработки, или возражения против указанной обработки;  - о праве подачи жалобы в надзорный орган;  - об источнике любой доступной информации, связанной с персональными данными, если они получены не от субъекта данных;  - о применении автоматизированного способа принятия решения, в том числе составление профиля, а также, по крайней мере в этих случаях, достоверной информации об имеющем место алгоритме, также как о значимости и предполагаемых последствиях обработки для субъекта данных;  - о передаче персональных данных на территорию Российской федерации с указанием гарантий выполнения прав физических лиц и защиты их персональных данных согласно standard contract clauses.  2. Рекомендуется реализовать функционал, при котором работники Лицензиата, будут иметь возможность выгрузить свои персональные данные и данные своих Клиентов в машиночитаемом виде в формате XML, JSON, CSV.  3. Рекомендуется внедрить процесс по реализации данного права субъектов данных по GDPR работниками Контроллера в соответствии с документом Subject Access Requests General Guidance. |
| 1.18. | Выполнение прав субъектов персональных данных на исправление персональных данных | article 16 GDPR | В локальных документах Контроллера и документе Privacy Policy не отображено право субъектов данных на исправление персональных данных и не регламентированы шаги по исправлению обработки персональных данных.  При этом в сервисе Yclients реализован функционал по исправлению своих персональных данных работниками Лицензиата. | ВЧ | 1. Рекомендуется в документах Privacy Policy и Subject Access Requests General Guidance прописать возможность реализации права субъектов данных на исправление своих персональных данных.  2. Рекомендуется внедрить процесс по реализации данного права субъектов данных по GDPR работниками Контроллера в соответствии с документом Subject Access Requests General Guidance. |
| 1.19. | Выполнение прав субъектов персональных данных на удаление персональных данных (право на забвение) | article 17 GDPR | В локальных документах Контроллера и документе Privacy Policy не отображено право субъектов данных на удаление персональных данных и не регламентированы шаги по удалению обработки персональных данных. | НВ | 1. Рекомендуется в документах Privacy Policy и Subject Access Requests General Guidance прописать возможность реализации права субъектов данных на удаление своих персональных данных.  2. В документах Privacy Policy и Subject Access Requests General Guidance рекомендуется указать, что данные не могут быть удалены, если обработка персональных данных требуется:  - для осуществления права на свободу выражения мнения и распространения информации;  - для соблюдения правовой обязанности, которая требует обработки в соответствии с правом Евросоюза или для выполнения задачи, осуществляемой в общественных интересах, либо при осуществлении официальных полномочий, возложенных на Контроллера;  - в силу общественных интересов в сфере социального здравоохранения;  - для архивных целей в общественных интересах, научных или исторических исследовательских целях, либо для статистических целей;  - для предъявления, исполнения или защиты правовых притязаний Контроллера.  1. Рекомендуется использовать сервисы для отзыва согласий и удаления персональных данных посетителей сайтов, например<https://www.cookiebot.com/>.  2. Рекомендуется внедрить процесс по реализации данного права субъектов данных по GDPR работниками Контроллера в соответствии с документом Subject Access Requests General Guidance.  3. Рекомендуется реализовать возможность полного удаления аккаунта в сервисе Yclients по просьбе субъекта данных. |
| 1.20. | Выполнение права субъекта данных на ограничение обработки персональных данных | article 18 GDPR | В локальных документах Контроллера и документе Privacy Policy не отображено право субъектов данных на ограничение обработки персональных данных и не регламентированы шаги по ограничению обработки персональных данных. | НВ | 1. Рекомендуется в документах Privacy Policy и Subject Access Requests General Guidance прописать возможность реализации права физических лиц на ограничение обработки своих персональных данных, а именно отобразить следующие случаи, когда он может воспользоваться этим правом:  - точность персональных данных оспаривается субъектом данных, в течение срока, позволяющего Контроллеру проверить точность персональных данных;  - обработка является неправомерной, и субъект данных возражает против удаления персональных данных, и взамен требует ограничить их использование;  - Контроллеру больше не нужны персональные данные для целей обработки, но они требуются субъекту данных для предъявления, исполнения или защиты правовых притязаний;  - субъект данных возражал против обработки в соответствии автоматизированным принятием решений на основании обработки его персональных данных, ожидая удостоверения того, преобладают ли правовые основания Контроллера таким правовым основаниям субъекта данных.  2. Рекомендуется прописать в документах Privacy Policy и Subject Access Requests General Guidance, что персональные данные могут далее обрабатываться для предъявления, исполнения или защиты правовых притязаний, или для защиты прав другого физического или юридического лица, либо по причинам важного общественного интереса Евросоюза.  3. Рекомендуется реализовать возможность обезличивания персональных данных пользователей личных кабинетов в сервисе Yclients через интерфейс с возможностью прекращения ограничения обработки персональных данных в дальнейшем пользователем самостоятельно. Для этого данные должны обезличиваться с генерацией ключа (набор символов или файл), которые будут выгружаться пользователю при активации процедуры обезличивания. При прекращении ограничения обработки персональных данных пользователь должен иметь возможность подгрузить в интерфейс ранее полученный ключ, при этой процедуре должен восстановиться доступ к его аккаунту и персональным данным.  4. Рекомендуется внедрить процесс по реализации данного права субъектов данных по GDPR работниками Контроллера в соответствии с документом Subject Access Requests General Guidance. |
| 1.21. | Выполнение обязательства по уведомлению в отношении исправления или удаления их персональных данных или ограничении обработки персональных данных | article 19 GDPR | В локальных документах Контроллера и документе Privacy Policy не отображена информация об уведомлении в отношении исправления или удаления их персональных данных или ограничении обработки персональных данных субъектов данных. | НВ | 1. Рекомендуется в документах Privacy Policy и Subject Access Requests General Guidance прописать информацию об уведомлении субъектов об удалении их персональных данных и дополнить информаций об информировании об ограничении обработки персональных данных и о том, что Контроллер прилагает все меры, направленные на удаление и ограничение обработки процессорами и третьими лицами персональных данных, переданных им Контроллером.  2. Рекомендуется внедрить процесс по реализации данного права субъектов данных по GDPR согласно документа Subject Access Requests General Guidancах |
| 1.22. | Выполнение права субъекта данных на переносимость его персональных данных (right of data portability) | article 20 GDPR | В локальных документах Контроллера и документе Privacy Policy не отображена информация о реализации прав для субъектов данных о переносимости их персональных данных. | НВ | 1. Рекомендуется в документе Privacy Policy и прописать возможность реализации субъектами данных права на переносимость своих персональных данных в случаях, когда персональные данные обрабатываются на основании согласия или договора. Выгрузке подлежат все персональные данные работников и клиентов Лицензиата.  2. Рекомендуется реализовать функционал, при котором работники Лицензиата, будут иметь возможность выгрузить свои персональные данные и данные своих Клиентов в машиночитаемом виде в формате XML, JSON, CSV.  3. Рекомендуется прописать в документе, описывающем реализацию прав субъектов данных внутри Контроллера (Subject Access Requests General Guidance), реализацию права на переносимость персональных данных работниками Контроллера.  4. Рекомендуется внедрить процесс по реализации данного права субъектов данных по GDPR работниками Контроллера в соответствии с документом Subject Access Requests General Guidance. |
| 1.23. | Выполнение права субъекта данных на возражение обработке персональных данных | article 21 GDPR | В Privacy Policy Контроллера не отображена информация о возможности реализации прав субъектов данных на возражение обработке персональных данных.  Также Контроллером не регламентирована процедура реализации такого права своими работниками. | НВ | 1. Рекомендуется описать в документе Privacy Policy возможность субъектов данных воспользоваться правом на возражение обработке персональных данных с указанием конкретных автоматических методов такой реализации.  2. Рекомендуется прописать в документе, описывающем реализацию прав субъектов данных внутри Контроллера (Subject Access Requests General Guidance), реализацию права на возражение обработке персональных данных работниками Контроллера.  3. Рекомендуется использовать сервисы для отзыва согласия и удаления cookie посетителей сайтов, например<https://www.cookiebot.com/>.  4. Рекомендуется внедрить процесс по реализации данного права субъектов данных по GDPR работниками Контроллера в соответствии с документом Subject Access Requests General Guidance. |
| 1.24. | Выполнение требований при автоматизированном индивидуальном принятии решения, включая профилирование | article 22 GDPR | У Контроллера отсутствует автоматизированное индивидуальное принятие решения в отношении субъекта данных при обработке его персональных данных, при котором осуществляется решение, серьезно влияющие на субъекта данных. | ВП |  |
| **2.** | Требования, неисполнение или нарушение которых ведет к штрафам в размере до 10 млн евро или 2% общегодового мирового оборота компании | | | | |
| 2.1. | Требования, неисполнение или нарушение которых ведет к штрафам в размере до 10 млн евро или 2% общегодового мирового оборота компании | article 8 GDPR | В документе Privacy Policy Контроллера не описана позиция Контроллера по обработке персональных данных несовершеннолетних. | НВ | Рекомендуется добавить в документ Privacy Policy запрет на использование сервисов Контроллера несовершеннолетними и указать сроки наступления совершеннолетия в странах присутствия Партнеров и Интеграторов. |
| 2.2. | Выполнение условий по идентификации субъекта персональных данных | article 11 GDPR | У Контроллера не установлена процедура идентификации субъекта данных для реализации ими своих прав в случае недостаточного количества данных для его идентификации. | НВ | 1. Рекомендуется проверять идентификацию физического путем запроса у него дополнительной идентификационной информации (номер телефона, идентификационного номера, сведений о последних 1-3 записях на услуги Лицензиатов) и путем направления письма и смс с ссылкой подтверждения, переход по которой будет являться идентификацией человека.  2. Рекомендуется добавить в документ, описывающий исполнение прав субъектов данных (Subject Access Requests General Guidance), информацию о случаях, когда будет требования идентификация субъекта данных и сведения о способах такой идентификации. |
| 2.3. | Выполнение требований по защите данных по умолчанию и при проектировании | article 25 GDPR | При проектировании нового или изменении имеющегося процесса обработки персональных данных или информационной системы, Контроллер не проводит процедуру оценки возможной минимизации обрабатываемых персональных данных и не анализирует их на предмет возможных рисков для субъектов данных.  На момент проведения обследования Контроллер не применял требований обеспечения конфиденциальности по умолчанию и при проектировании («privacy by design» и «privacy by default»). | НВ | 5. Рекомендуется провести процедуру DPIA для информационной системы Yclients и связанных с ней бизнес процессов.  6. После проведения процедуры DPIA рекомендуется применять выбранные для минимизации рисков для субъектов данных организационные и технические меры безопасности персональных данных.  7. Рекомендуется уменьшать количество персональных данных собираемых о субъектах данных, если это не будет вредить бизнес-процессам и бизнесу Контроллера.  8. Рекомендуется при проектировании новых информационных систем или изменении текущих, в т.ч. связанных с ними процессов обработки персональных данных проводить, процедуру минимизации обрабатываемых персональных данных и DPIA.  9. Рекомендуется при проектировании новых информационных систем или изменения имеющихся применять по умолчанию шифрование или псевдонимизацию персональных данных. |
| 2.4. | Выполнение требований при совместной обработке персональных данных с другими контроллерами | article 26 GDPR | У Контроллера не выявлена совместная обработка персональных данных с другими контроллерами. | ВНТ |  |
| 2.5. | Наличие представителя в ЕС | article 27 GDPR | На территории стран-членов Евросоюза, где Контроллер через Партнеров и Агентов осуществляет свою деятельность, не назначен обязательный представитель в ЕС. | НВ | 1. Рекомендуется назначить одного представителя в ЕС на территории одного из европейских государств, где Контроллер через Партнеров и Интеграторов ведет свою деятельность.  2. Представителем в ЕС может являться юридическое или физическое лицо, являющееся резидентом одной и стран-членов ЕС.  3. Рекомендуется заключить с выбранным представителем двуязычное (один язык русский, второй официальный язык страны присутствия представителя) соглашение о предоставлении интересов Контроллера по GDPR на территории ЕС.  4. В заключаемом соглашении рекомендуется прописать:  - обязанность представителя незамедлительно передавать Контроллеру поступающие запросы от надзорных органов по защите данных из ЕС, физических лиц и контрагентов;  - обязанность незамедлительно передавать от Контроллера ответы на поступающие запросы надзорным органам по защите данных из ЕС, физическим лицам и контрагентам;  - обязанность Контроллера возместить представителю в ЕС штрафы, наложенные на представителя по вине Контроллера. |
| 2.6. | Поручение персональных данных на обработку обработчику | article 28 GDPR | Котроллер передает или поручает персональные данные физических лиц, находящихся на территории ЕС, на обработку Партнерам и Интеграторам с территории стран-членов ЕС, а также третьим лицам и сервисам, находящимся на территории ЕС (Hetzner), Российской Федерации (ООО «Таймпэд Лтд», сервисом Sipuni, сервисом AmoCRM и хостинг-провайдером Servers.ru) и на территории США (Zendesk, Intercom, Slack).    Также Контроллер осуществляет обработку персональных данных физических лиц, находящихся на территории ЕС и порученных ему на обработку Лицензиатами.  При этом Контроллер не заключил с вышеуказанными лицами обязательные соглашения, необходимые при передаче и поручении персональных данных. | НВ | 1. Рекомендуется разработать 3 шаблона документа Data Processing Agreement (далее – DPA) на базе утвержденных Еврокомиссией Standard contractual clauses для подписания с:  - Лицензиатами с территории стран-членов ЕС;  - Партнерами и Интеграторами с территории стран-членов ЕС;  - с третьими лицами и сервисами, находящимися на территории Российской Федерации (ООО «Таймпэд Лтд», сервисом Sipuni, сервисом AmoCRM и хостинг-провайдером Servers.ru).  2. Документы DPA могут быть подписаны в бумажном виде или в электронном с подписанием документа электронной подписью в соответствии с законодательством ЕС. Документы рекомендуется подписывать двуязычными, одним из языков должен быть русский, а вторым язык юридического лица, с кем подписывается DPA.  3. Рекомендуется связаться с сервисами, находящимися в США и на территории ЕС (Zendesk, Intercom, Slack, Hetzner), чтобы уточнить у них возможность подписания с ними DPA и запросить для подписания их шаблон DPA.  4. В случае невозможности подписания с сервисами из предыдущего пункта DPA, рекомендуется написать им о нарушении требований GDPR о необходимости подписания DPA или найти аналогичные сервисы, готовые подписать DPA.  5. В разрабатываемых DPA отражать следующую информацию:  - гарантии того, что процессор обрабатывает персональные данные только на основании документально подтвержденных распоряжений Контроллера, в том числе в отношении передачи персональных данных третьей стране или международной организации, если только этого не требует право Евросоюза или право государств-члена Евросоюза, которое применяется к процессору; в этом случае процессор должен проинформировать Контроллера об этих правовых требованиях до начала обработки, за исключением случаев, когда такое право запрещает подобное информирование по основаниям общественного интереса;  - гарантии процессора, что лица, уполномоченные обрабатывать персональные данные, взяли на себя обязательства соблюдать конфиденциальность, либо эти обязательства соблюдать конфиденциальность уже предусмотрены законом;  - принятие процессором всех мер по обеспечению безопасности персональных данных;  - соблюдение условий процессором по привлечению другого процессора;  - принимая во внимание характер обработки, помощь Контроллеру соответствующими техническими и организационными мерами, насколько это возможно, осуществлять обязанности Контроллера отвечать на запросы по осуществлению прав субъекта данных;  - информация о содействии Контроллеру в обеспечении соблюдения обязанностей̆ в соответствии со Статьями 32-36 GDPR, принимая во внимание характер обработки, а также информацию, доступную для процессора;  - по выбору Контроллера, гарантии удаления или возвращения всех персональных данных Контроллеру по завершению предоставления услуг, связанных с обработкой̆, а также удаления существующих копий, кроме случаев, когда право Евросоюза или право государства-члена требует хранения персональных данных;  - обязательство о предоставлении в распоряжение Контроллера всей информации, необходимой для того, чтобы подтвердить соблюдение обязанностей̆, предусмотренных в DPA, а также дающую возможность и содействующую проведению аудита, включая инспекционные проверки, проводимые Контроллером либо иным аудитором, уполномоченным Контроллером. |
| 2.7. | Требование по ограничению обработки персональных данных процессором в иных целях, кроме тех, которые установлены контроллером, правом ЕС или государств-членов ЕС | article 29 GDPR | Прописанное ограничение обработки в заявленных целях отсутствует в договорах, подписываемых с Лицензиатами и партнерами. | НВ | Рекомендуется явно прописать в документах DPA, заключаемых с Лицензиатами, Партнерами и Интеграторами, с третьими лицами и сервисами, находящимися на территории Российской Федерации, ЕС и США, что персональные данные должны обрабатываться только в описанных в документе целях, будут удаляться по истечении таких целей или разрыва договора, и не будут обрабатываться в иных целях. |
| 2.8. | Ведение учета обработки персональных данных | article 30 GDPR | Контроллер является процессором по отношению к персональным данным, поручаемым ему на обработку Лицензиатами, в связи с чем необходимо вести учет обрабатываемых персональных данных по поручению.  При этом у Контроллера работает менее 250 работников, в связи с чем не требуется проводить учет персональных данных. | ВНТ | В качестве применения лучшей практики и прозрачного взаимодействия с надзорными органами по защите данных на территории стран-членов ЕС, рекомендуется составить документ Data Inventory, в который будет входить следующая информация:  - имя и контактные данные Контроллера, каждого Лицензиата, от имени которого процессор действует, и, где это применимо, представителя Контроллера, а также контакты ответственного за защиту данных;  - категории обработки персональных данных физических лиц из стран-членов ЕС, осуществляемой от имени Лицензиатов;  - о передаче таких персональных данных, когда это применимо, в третью страну или международную организацию, включая указание этой третьей страны или международной организации, а в случае передачи персональных данных документальное подтверждение надлежащего обеспечения защиты;  - общее описание технических и организационных мер безопасности. |
| 2.9. | Сотрудничество с надзорным органом | article 31 GDPR | У Контроллера не регламентирована процедура реагирования на запросы надзорных органов стран-членов ЕС в области защиты данных.  Запросов от надзорных органов по GDPR Контроллеру не поступало. | НВ | Рекомендуется разработать внутренний документ, регламентирующий процедуру реагирования на запросы надзорных органов стран-членов ЕС в области защиты данных. |
| 2.10. | Обеспечение безопасности при обработке персональных данных | article 32 GDPR | При проектировании нового или изменении имеющегося процесса обработки персональных данных физических лиц, находящихся на территории ЕС, или информационной системы, в которой обрабатываются такие персональные данные, Контроллер не проводит процедуру оценки возможной минимизации обрабатываемых персональных данных («privacy by default») и не анализирует такие изменения на предмет возможных рисков для субъектов данных («privacy by default»).  Контроллером не проводилась процедура Data Protection Impact Assessment для определения рисков для субъектов данных и мер (контролей) по их снижению. | НВ | 1. Рекомендуется провести процедуру DPIA для имеющихся информационных систем и процессов обработки, в которой обрабатываются персональные данные физических лиц, находящихся на территории ЕС (информационная система Yclients и процессы обработки, связанные с ней).  2. Рекомендуется проводить процедуру DPIA для каждой новой информационной системы (продукте), в которой обрабатываются персональные данные физических лиц из ЕС, и для новых процессов обработки персональных данных.  3. После проведения процедуры DPIA рекомендуется применять выбранные для минимизации рисков для субъектов данных организационные и технические меры безопасности персональных данных.  4. Рекомендуется на ежегодной основе проводить аудит безопасности персональных данных сторонней организацией.  5. Рекомендуется разработать внутренний документ, регламентирующий обеспечение безопасности персональных данных у Контроллера в соответствии с GDPR (IT Security Policy). |
| 2.11. | Уведомление надзорного органа об утечке персональных данных | article 33 GDPR | В рамках предоставленной информации у Контроллера не выявлено прецедентов утечек персональных данных, но у Контроллера не определена процедура уведомления надзорных органов ЕС об утечке персональных данных и не разработан соответствующий регламентирующий документ. | НВ | Рекомендуется разработать документ, регламентирующий процедуру уведомления об утечке персональных данных надзорного органа той страны, в которой будет находиться главное представительство Контроллера в ЕС (Data Breach Policy). |
| 2.12. | Информирование субъекта данных об утечке персональных данных | article 34 GDPR | В рамках предоставленной информации у Контроллера не выявлено прецедентов утечек персональных данных, но не определена процедура принятия мер для минимизации последствий утечек для субъектов данных, информирования субъекта данных об утечке персональных данных и не разработан соответствующий документ. | НВ | Рекомендуется разработать документ, регламентирующий процедуру принятия мер для минимизации последствий утечек для субъектов данных и информирование субъектов данных об утечке персональных данных и принятых мерах (Data Breach Policy). |
| 2.13. | Проведение оценки воздействия на защиту персональных данных (DPIA) | article 35 GDPR | Контроллер не осуществляет систематический мониторинг действий пользователей в широких масштабах, что может привести к высокому риску для прав и свобод субъектов данных, и обработка данных не несет высокий риск для субъектов данных. Но при этом Контроллер является разработчиком программного обеспечения, которое предоставляется в пользование Лицензиатам, являющихся юридическими лицами и имеющими возможность запрашивать результаты проведения DPIA.  Контроллер не проводил процедуру DPIA на момент проведения обследования. | НВ | 1. Рекомендуется провести процедуру DPIA для информационной системы Yclients и всех процессов обработки персональных данных, предусмотренных в ней. Результаты проведения DPIA должны быть задокументированы.  2. За основу для проведения процедуры DPIA рекомендуется применять рекомендации французского надзорного органа по защите данных, CNIL, или использовать Методику определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена 14 февраля 2008 г. заместителем директора ФСТЭК России).  3. Результаты DPIA должны быть учтены в Data Inventory по тем процессам, для которых проводилась данная процедура.  4. Рекомендуется вести реестр проведенных процедур DPIA. |
| 2.14. | Обязательное предварительное консультирование с надзорным органом при наличии высокого риска для субъектов данных | article 36 GDPR | Контроллер не проводил процедуру DPIA, в связи с чем отсутствует информация по уровню риска для субъектов данных и отсутствует понимание о необходимости проведения такой консультации с надзорным органом. | НВ | Рекомендуется провести процедуру DPIA и осуществить переоценку соответствия по данному требованию. |
| 2.15. | Назначение инспектора по защите персональных данных (DPO) | article 37-39 GDPR | Контроллер не является государственным органом одной из стран-членов Евросоюза или органом, исполняющим распоряжения судов.  Контроллер не обрабатывает чувствительные персональные данные или сведения, касающиеся уголовных приговоров и преступлений, а также не осуществляет регулярного и систематического мониторинга субъектов данных в больших масштабах для осуществления основной деятельности, т.к. основная деятельность Контроллера заключается в разработке программного обеспечения и предоставления неисключительных прав на его использование.  В связи с вышеизложенным назначение инспектора по защите персональных данных не требуется. | ВНТ | Рекомендуется в качестве лучшей практики назначить в организации ответственного за защиту данных или заключить договор со сторонней организацией, в обязанности которых будет входить:  1. информирование и консультирование Контроллера и его работников, выполняющих обработку своих обязательств в соответствии с GDPR;  2. контроль соблюдения GDPR, а также политики Контроллера в отношении защиты персональных данных, включая распределение обязанностей, повышение осведомленности и обучение работников, участвующего в операциях по обработке данных, и проведение соответствующих аудитов;  3. предоставление консультаций по запросу в отношении оценки воздействия защиты данных (DPIA);  4. сотрудничество с контролирующими органами в области защиты прав субъектов данных в странах-членах ЕС;  5. выступление в качестве контактного лица для контролирующего органа по вопросам, касающимся обработки, включая предварительные консультации. |
| 2.16. | Выполнение требований при передаче персональных данных в третьи страны | Chapter 5 GDPR | Персональные данные физических лиц, находящихся на территории ЕС, а именно работников Лицензиата, клиентов Лицензиата, работников компаний партнеров, участников мероприятий и физических лиц, обратившихся через форму обратной связи, обрабатываются работниками Контроллера, расположенными на территории Российской Федерации, которая не является доверенной страной, обеспечивающей адекватную защиту прав субъектов данных согласно GDPR. Также Контроллер организует передачу персональных данных вышеуказанных субъектов персональных данных в информационные системы Zendesk, Intercom, Slack и AmoCRM, которые располагаются на территории США, которая не является доверенной страной, обеспечивающей адекватную защиту прав субъектов данных согласно GDPR.  Контроллером передаются персональные данные участников передаются ООО «Таймпэд Лтд», которое располагаются на территории Российской Федерации.  При этом Контроллером не реализованы методы защиты прав субъектов данных на территории США и субъекты данных не уведомлены о трансграничной передаче персональных данных на территорию России и США. | НВ | Для приведения процессов обработки персональных данных в соответствие в части передачи персональных данных на территорию третьих стран, не обеспечивающих адекватную защиту прав субъектов согласно GDPR, рекомендуется:  1. Разработать, опубликовать в Privacy Policy и добавить в дополнительным соглашением в договора с партнерами и лицензиатами утвержденные Еврокомиссией Standard contractual clauses, по которому Контроллер продемонстрирует безопасность передачи персональных данных на территорию Российской Федерации и США с описанием выполняемых мер для защиты персональных данных. Не рекомендуется применения еще одного легитимного способа, согласий субъектов данных на передачу персональных данных на территорию Российской Федерации и США, на сайтах и в продуктах Контроллера в связи с возможным снижением конверсии.  2. Рекомендуется заключить дополнительное соглашение с ООО «Таймпэд Лтд», сервисом Sipuni, сервисом AmoCRM и хостинг-провайдером Servers.ru, в котором продублировать основные положения утвержденных Еврокомиссией Standard contractual clauses.  3. Рекомендуется связаться с сервисами Zendesk, Intercom и Slack для обсуждения возможности заключения с ними Standard contractual clauses.  4. В дальнейшем, при расширении бизнеса Контроллера на территории ЕС с учреждением юридических лиц, рекомендуется разработать и согласовать с выбранным надзорным органом в области защиты персональных данных обязательные корпоративные правила (Binding corporate rules, BCR). Данный документ позволяет обмениваться между юридическими лицами Контроллера по всему миру персональными данными субъектов данных из ЕС без необходимости подписания между собой отдельных договоров. Срок согласования BCR с надзорным органом составляет от 6 до 12 месяцев. |

[1] НВ – не выполнено, ВЧ – выполнено частично, ВП – выполнено полностью, ВНТ – выполнение не требуется