**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

на оказание услуг по комплексному обследованию процессов обработки персональных данных для определения степени соответствия требованиям Федерального закона от 27.07.2006 №152-ФЗ "О персональных данных" и актуализации документации по обработке и защите персональных данных Заказчика.

1. **Предмет договора**

Услуги по комплексному обследованию процессов обработки персональных данных для определения степени соответствия требованиям Федерального закона от 27.07.2006 №152-ФЗ "О персональных данных" и актуализации документации по обработке и защите персональных данных Заказчика.

1. **Заказчик: ООО «ФРИИ Инвест».**
2. **Общие требования к оказанию услуг**

3.1 Место оказания услуг: услуги оказываются по месту нахождения Заказчика по адресу: 101000, г. Москва, ул. Мясницкая, д. 13, стр. 18.

3.2 Планируемое количество сотрудников для проведения интервью: не менее 20.

3.3 Перечень ИС: не менее (но не ограничиваясь) 20 информационных систем, включая предоставляемые головной организацией.

3.4 Срок оказания услуг: не более 100 (ста) рабочих дней с даты заключения договора.

**3.5 Перечень услуг и требования к результату оказания услуг**

Услуги оказываются поэтапно:

**3.5.1 ЭТАП 1**

**Проведение комплексного обследования текущего состояния организации в области обработки персональных данных.**

Данный этап включает в себя следующие подэтапы, выполняемые последовательно:

* Определение основных видов деятельности Заказчика;
* Изучение его организационной структуры с целью выявления подразделений, функциональное назначение которых предполагает осуществление обработки персональных данных;
* Обследование информационных систем и процессов обработки персональных данных;
* Определение необходимости актуализации уведомления об обработке персональных данных в Роскомнадзор;
* Определение случаев несоответствия требованиям Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных". Обследование информационных систем и процессов обработки персональных данных;

**Обследование информационных систем и процессов обработки персональных данных:**

Определяются основные виды деятельности Заказчика и изучается его организационная структура с целью выявления подразделений, функциональное назначение которых, предполагает осуществление обработки персональных данных, а также разработки анкет и плана интервьюирования сотрудников с учетом специфики Заказчика.

**В ходе выполнения обследования информационной инфраструктуры и объектов автоматизации Исполнитель осуществляет следующие действия:**

* выявление процессов обработки персональных данных, в том числе определение процедур сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления и уничтожения персональных данных;
* определение способов обработки персональных данных (автоматизированная, неавтоматизированная) и программно-технических средств, используемых для обработки персональных данных;
* определение целей обработки персональных данных;
* определение перечня сотрудников (подразделений), участвующих в обработке персональных данных;
* выявление сторонних организаций (третьих лиц), в том числе государственных регулирующих органов, в рамках отношений, с которыми осуществляется передача им или получение от них персональных данных;
* определение категорий физических лиц (субъектов персональных данных), чьи персональные данные обрабатываются;
* определение перечня и объема обрабатываемых персональных данных;
* определение документов, собираемых с физических лиц и содержащих персональные данные;
* анализ договоров, соглашений, согласий, публичных оферт и иных документов, заключаемых с третьими лицами, в рамках отношений, с которыми осуществляется передача им или получение от них персональных данных;
* анализ договоров, соглашений, согласий, публичных оферт и иных документов, заключаемых с физическими лицами и являющихся основаниями для обработки персональных данных;
* определение мест хранения носителей, содержащих персональные данные;
* определение адресов офисов и помещений, в которых осуществляется обработка персональных данных;
* выделение прикладных информационных систем, в которых обрабатываются персональные данные;
* определение спецификации серверного сегмента и рабочих станций, входящих в состав информационных систем персональных данных;
* определение схем физического подключения и логического взаимодействия компонентов информационных систем персональных данных, схем подключения к сетям связи общего пользования и международного информационного обмена с определением пропускной способности линий связи;
* описание используемого комплекса средств защиты персональных данных и механизмов идентификации, аутентификации и разграничения прав доступа пользователей информационных систем персональных данных на уровне операционных систем, баз данных и прикладного программного обеспечения;
* определение наличия организационно-распорядительной документации, определяющей порядок обработки и защиты персональных данных;
* описание физических мер защиты персональных данных, в том числе выделенной контролируемой зоны, организации пропускного режима, системы резервного электропитания и прочее;
* определение месторасположения баз данных, содержащих персональные данные;
* выявление фактов трансграничной передачи персональных данных и составление перечня стран, куда осуществляется трансграничная передача персональных данных.

**Отчетные документы**

Отчетными документами по данному этапу являются:

* Согласованный Заказчиком Аналитический отчёт «Результаты обследования процессов обработки и обеспечения безопасности ПДн», включающий в себя помимо прочего следующие приложения:
	+ Приложение 1. Перечень подразделений и лиц, допущенных к работе с обрабатываемыми ПДн.
	+ Приложение 2. Перечень обрабатываемых ПДн;
	+ Приложение 3. Перечень сторонних организаций (третьих лиц), в том числе государственных регулирующих органов, в рамках отношений, с которыми осуществляется передача им или получение от них персональных данных;
	+ Приложение 4. Перечень ИСПДн Заказчика.
	+ Приложение 5. Оценка степени выполнения требований законодательства РФ

**Определение необходимости актуализации уведомления:**

На основании анализа отношений с субъектами персональных данных, категорий и способов обработки персональных данных при наличии устаревших сведений в существующем уведомлении сведения актуализируются.

**Отчетные документы**

Отчетными документами по данному этапу являются:

Информационное письмо о внесении изменений в сведения в реестр операторов, осуществляющих обработку персональных данных.

**Определение степени несоответствия требованиям Федерального закона от 27.07.2006 N 152-ФЗ "О ПЕРСОНАЛЬНЫХ ДАННЫХ"**

На основании проведенного обследования информационных систем и процессов обработки определяется степень несоответствия требованиям Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" в части обработки персональных данных.

По итогам определения степени несоответствия подготавливаются рекомендации по приведению информационных систем, процессов обработки и документационного обеспечения в соответствие законодательству Российской Федерации в области персональных данных.

**Отчетные документы**

Отчетными документами по данному этапу являются:

Перечень несоответствий требованиям законодательства Российской Федерации в области персональных данных и рекомендаций по их устранению.

**Отчетные документы и промежуточный акт об оказании услуг по этапу 1 предоставляются в электронном виде с обязательным дублированием на бумажном носителе не позднее 5 рабочих дней после окончания срока оказания услуг по этапу.**

**3.5.2 ЭТАП 2**

 **Разработка моделей угроз, определение вероятного ущерба и уровней защищенности персональных данных при их обработке в информационных системах персональных данных:**

На основании информации Этапа 1 производится разработка документов «Модель угроз безопасности персональных данных, обрабатываемых в информационной системе персональных данных» для каждой определенной информационной системы персональных данных и проведение процедур по определению уровней защищенности персональных данных, обрабатываемых информационных систем персональных данных. Исходя из определенных уровней защищенности персональных данных определяются меры по обеспечению безопасности персональных данных исходя из требований Приказа ФСТЭК России от 18.02.2013 N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных".

Постановления Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"

Приказа ФСБ России от 10 июля 2014 г. N 378 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности".

**Этап 2 включает:**

* Разработку и актуализацию документов «Модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» для всех ИСПДн выявленных на Этапе 1;
* Определение вероятного ущерба для Заказчика, субъектов ПДн;
* Определение уровней защищенности персональных данных при их обработке в информационных системах персональных данных;

**Актуализация документов «Модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных»:**

На основании экспертной оценки актуальности угроз в условиях функционирования информационных системах персональных данных для каждой системы формируется модель угроз безопасности персональных данных.

**При разработке новых редакций моделей угроз учитываются требования:**

* Постановления Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";
* «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;
* «Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

В случае использования в информационных системах персональных данных средств криптографической защиты информации при разработке моделей угроз дополнительно учитываются положения «Методических рекомендаций по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности от 31 марта 2015 г. № 149/7/2/6-432».

**Отчетные документы**

Отчетными документами по данному этапу являются согласованные с Заказчиком новые редакции документов:

* «Модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных» для каждой информационной системы персональных данных;

**Определение уровней защищенности персональных данных при их обработке в информационных системах персональных данныx:**

Для определения уровня защищенности персональных данных производится анализ категорий и объема обрабатываемых персональных данных в информационных системах (согласно Перечня ИСПДн), категорий субъектов персональных данных кому они принадлежат и типов актуальных угроз.

По результатам проведенных работ готовятся проекты актов определения уровней защищенности персональных данных для каждой информационной системы персональных данных.

**Отчетные документы**

Отчетными документами по данному этапу являются новые редакции документов:

* «Акт определения уровней защищенности персональных данных при их обработке в информационной системе персональных данных» для каждой информационной системы персональных данных.

Документы предоставляются с промежуточным актом об оказании услуг по Этапу 2.

**3.5.3 ЭТАП 3**

**Актуализация организационно-распорядительной документации:**

Актуализация организационно-распорядительной документации позволяет закрыть ряд требований, предъявляемых как к автоматизированной обработке персональных данных, так и к обработке персональных данных без использования средств автоматизации.

При актуализации организационно-распорядительной документации проводится синтез требований различных нормативно-правовых актов в области персональных данных с целью структурирования содержания комплекта организационно-распорядительной документации для наиболее эффективного его применения, дальнейшей актуализации и обновления.

**Отчетные документы**

Отчетными документами по данному этапу являются следующие новые редакции документов:

1. План мероприятий по приведению в соответствие требованиям законодательства в области персональных данных;
2. Приказ о назначении лиц, ответственных за обработку и защиту персональных данных, и утверждении документов по персональным данным
3. Политика Оператора в отношении обработки персональных данных (количество в соответствии с Отчетом)
4. Положение по организации обработки и обеспечению безопасности персональных данных
5. Инструкция ответственного за организацию обработки персональных данных
6. Перечень процессов обработки персональных данных и сведения об их обработке, включающий как минимум следующую информацию:
	* Категория субъекта
	* Цель обработки
	* Подразделение(лицо), ответственное за обработку
	* Категории данных
	* Правовая основа
	* Действия с ПДн
	* В каком виде собирается согласие
	* Третьи лица, которым передаются ПДн
	* Третьи лица, которые ведут обработку по поручению
	* Срок прекращения обработки
	* ИСПдн в которой ведется обработка
7. Перечень информационных систем персональных данных;
8. Перечень должностей и третьих лиц, допущенных к обработке персональных данных;
9. Форма Обязательства о неразглашении персональных данных;
10. Согласия на обработку персональных данных (количество в соответствии с Отчетом по Этапу 1), включая Согласия на обработку персональных данных разрешенных субъектом персональных данных для распространения
11. Соглашения об обеспечении безопасности персональных данных, порученных на обработку - Соглашения о поручении обработки персональных данных (количество в соответствии с Отчетом)
12. Акт оценки вреда, который может быть причинен субъектам, персональные данные которых обрабатываются Оператором
13. Акт определения уровня защищенности персональных данных, обрабатываемых в информационной системе персональных данных
14. Перечень помещений для обработки персональных данных;
15. Порядок получения доступа к ресурсам ИСПДн
16. Порядок организации парольной защиты в информационных системах персональных данных
17. Порядок обеспечения сетевой безопасности в Компании
18. Порядок предоставления удаленного доступа
19. Порядок установки, обновления и защиты программного обеспечения
20. Порядок использования мобильных технических средств в информационных системах персональных данных
21. Перечень программного обеспечения и (или) его компонентов, разрешенного к использованию на ПЭВМ, входящих в состав ИСПДн
22. Порядок изменения состава и конфигурации технических и программных средств в информационных системах персональных данных
23. Порядок защиты информации о событиях безопасности в информационных системах персональных данных
24. Порядок организации антивирусной защиты в информационных системах персональных данных
25. Положение о безопасной эксплуатации технических средств обработки, хранения и передачи ПДн в ИСПДн
26. Приказ об установлении границ контролируемой зоны
27. Регламент взаимодействия с регуляторами по информированию об инцидентах
28. Инструкция эксплуатации средств криптографической защиты
29. Регламент по учёту, хранению и уничтожению носителей персональных данных;
30. Регламент по допуску сотрудников и третьих лиц к обработке персональных данных;
31. Регламент по реагированию на запросы субъектов персональных данных;
32. Регламент по взаимодействию с органами государственной власти в области персональных данных;
33. Регламент по обезличиванию персональных данных;
34. Регламент по уничтожению персональных данных;

В случае выявления процессов, связанных с трансграничной передачей персональных данных:

1. Уведомление об осуществлении трансграничной передачи персональных данных;
2. Соглашение о трансграничной передаче персональных данных;
3. Регламент по трансграничной передаче персональных данных.

Документы предоставляются с промежуточным актом об оказании услуг по Этапу 3.

**3.5.4 Гарантийная поддержка:**

Гарантийная поддержка осуществляется в течение года с даты подписания акта об оказании услуг по Договору.

**Исполнитель обеспечивает:**

* Консультирование Заказчика и устранение замечаний к документации разработанной на Этапе 2,3 в случае выявления нарушений представителями Роскомнадзора во время проведения контрольно-надзорного мероприятия.

В случае, если в пределах сроков действия договора в отношении Заказчика проводятся контрольно-надзорные мероприятия со стороны Роскомнадзора, то в случае выявления нарушений представителями Роскомнадзора во время проведения контрольно-надзорного мероприятия в части документации разработанной на Этапе 2,3, специалисты Исполнителя помогают их устранить в сроки проведения контрольно-надзорного мероприятия.

В случае получения от представителей Роскомнадзора предписания об устранении выявленных нарушений в части документации разработанной на Этапе 2,3, специалисты Исполнителя помогают и консультируют в части устранения нарушений в сроки, указанные в предписании.

**4. Срок оказания услуг**

4.1 Общий срок оказания услуг по договору:

не более 100 рабочих дней с даты заключения договора.

4.2 Сроки оказания услуг по этапам

Этап 1 – не более 50 рабочих дней с даты заключения договора;

Этап 2 – не более 30 рабочих дней после приемки услуг по этапу 1;

Этап 3 – не более 20 рабочих дней после приемки услуг по этапу 2.

Работы по этапам могут проводиться одновременно.

**Гарантийная поддержка**: в течение года с даты подписания акта об оказании услуг по договору.

**5.Условия, порядок приема и сдачи оказанных услуг**

Разрабатываемые документы должны соответствовать требованиям действующего законодательства Российской Федерации, учитывать все выявленные и заявленные особенности обработки персональных данных, быть точными, взаимоувязанными и непротиворечивыми. Структура документов и их количество должны отвечать принципу модульности, т.е. позволять осуществление изменения, исключения, доработки отдельных документов, не затрагивая всего разрабатываемого пакета документов.

В процессе оказания услуг возможно изменение состава (перечня) и наименования документов, при обосновании таких изменений требованиями нормативных или методических документов и согласовании таких изменений с заказчиком.

Сдача проектов документов осуществляется путем предоставления в согласованный срок результата работ в электронной форме и в распечатанном виде.

По результатам Этапов № 1-3 составляются промежуточные акты о принятии услуг Заказчиком.

**6. Порядок оплаты**

Оплата осуществляется в течение 14 (Четырнадцати) рабочих дней с даты подписания Акта об оказании услуг по договору на основании счета Исполнителя.

**7.ТРЕБОВАНИЯ К ИСПОЛНИТЕЛЮ**

**Обязательные требования:**

7.1. Участник должен иметь подтвержденный опыт оказания услуг по предмету закупки не менее 5 лет. *Подтверждается Выпиской из ЕГРЮЛ.*

7.2. Суммарная выручка за 2021-2022гг. должна составлять не менее 50 млн. руб.

*Подтверждается копией финансовой отчетности за 2021-2022гг.: бухгалтерский баланс – форма 0710001 по ОКУД,*

 *- отчет о финансовых результатах – форма 0710002 по ОКУД.*

7.3. Наличие в штате не менее 1-го (одного) специалиста по информационной безопасности с соответствующим опытом работы не менее трех лет;

Наличие в штате не менее 1-го (одного) специалиста/эксперта в области персональных данных с соответствующим опытом работы не менее трех лет.

*Наличие сотрудников в штате и опыт работы подтверждается копиями трудовых договоров, трудовых книжек, приказов о приеме на работу, выпиской из штатного расписания*

*Квалификация подтверждается копиями дипломов, сертификатов об образовании.*

*Информация отражается в Форме 4 «Справка о кадровых ресурсах»*

7.4 Опыт участия в проверках Роскомнадзора.

*Подтверждается письмом от руководителя организации Заказчика об участии в проверках.*