**Часть  VI ТЕХНИЧЕСКАЯ ЧАСТЬ ЗАКУПОЧНОЙ ДОКУМЕНТАЦИИ**

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ НА ОКАЗАНИЕ КОНСУЛЬТАЦИОННЫХ УСЛУГ**

**ПО ОРГАНИЗАЦИИ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ ЗАКАЗЧИКОМ В СООТВЕТСТВИЕ ТРЕБОВАНИЯМ ЗАКОНОДАТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ**

1. **Общая информация**

Исполнитель оказывает Заказчику консультационные услуги по организации обработки и защиты персональных данных, обрабатываемых Заказчиком в соответствие требованиям законодательства Российской Федерации.

Перечень услуг и отчетные документы приведены в таблице

|  |  |  |
| --- | --- | --- |
| № | СТАДИЯ ОКАЗАНИЯ УСЛУГ | ОТЧЕТНЫЕ ДОКУМЕНТЫ  (на бумажном или электронном носителе) |
| 1 | Проведение комплексного обследования   * 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". | Протокол сбора информации  Заключение, подтверждающее статус выполнения требований к обработке персональных данных  Информационное письмо о внесении изменений в сведения в реестр операторов, осуществляющих обработку персональных данных (при необходимости)  Перечень несоответствий требованиям законодательства Российской Федерации в области персональных данных и рекомендаций по их устранению.  (при наличии несоответствий) |
| 2 | Проверка уровней защищенности персональных данных, обрабатываемых в информационных системах (не менее 12 информационных систем, согласно текущего Перечня ИСПДн), и актуализация требований по обеспечению безопасности персональных данных | Проект Акта определения уровней защищенности персональных данных при их обработке в информационной системе персональных данных |
| 3 | Актуализация организационно-распорядительной документации в соответствии с изменениями в законодательстве | Проекты новых редакций организационно-распорядительных документов Заказчика по перечню Приложения № 2 к Договору. |
| 4 | Гарантийная поддержка | Предоставляется Исполнителем в течении года, входит консультация актуализация организационно-распорядительной документации в соответствиями с изменениями в законе ФЗ-152 и изменениями в бизнес-процессах компании Заказчика. |

В рамках каждой стадии Исполнитель производит следующие действия

**СТАДИЯ 1: КОМПЛЕКСНОЕ ОБСЛЕДОВАНИЕ:**

Данная стадия включает в себя следующие этапы, выполняемые последовательно:

* 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:**

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 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:

* Протокол сбора информации
* Заключение, подтверждающее статус выполнения требований к обработке персональных данных

**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, степени несоответствия и рекомендаций по их устранению.

**СТАДИЯ 2: ПРОВЕРКА УРОВНЕЙ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ, И ФОРМИРОВАНИЕ ТРЕБОВАНИЙ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ:**

Производится актуализация 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".

**Стадия 2 должна включать три этапа:**

* Актуализация документов «Модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;
* Проверка уровней защищенности персональных данных при их обработке в информационных системах персональных данных;
* Актуализация требований по обеспечению безопасности 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:

* Новая редакция документа «Модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных» для каждой информационной системы персональных данных;
* Новая редакция документа «Протокол определения ущерба субъекту персональных данных» для каждой информационной системы персональных данных.

**ПРОВЕРКА 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 (не менее 12 информационных систем, согласно текущего 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:

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

**ФОРМИРОВАНИЕ ТРЕБОВАНИЙ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ:**

Данный этап включает работы по формированию отдельных требований к обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных, а также без использования средств автоматизации.

В данном случае, требования по обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных, разрабатываются для каждой системы, а интеграция требований осуществляется в документе «Рекомендации по совершенствованию системы защиты персональных данных».

**Отчетные документы**

Отчетными документами по данному этапу являются:

«Рекомендации по совершенствованию системы защиты персональных данных».

**СТАДИЯ 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 обновленные редакции документов:

1. Приказ о назначении комиссии по приведению в соответствие требованиям законодательства в области персональных данных;
2. Положение о комиссии по приведению в соответствие требованиям законодательства в области персональных данных;
3. План мероприятий по приведению в соответствие требованиям законодательства в области персональных данных;
4. Перечень должностей и третьих лиц, допущенных к обработке персональных данных;
5. Форма Обязательства о неразглашении персональных данных;
6. Форма Соглашения об обеспечении безопасности персональных данных, переданных на обработку;
7. Перечень обрабатываемых персональных данных;
8. Форма Согласия на обработку персональных данных;
9. Форма Согласия на передачу персональных данных третьему лицу;
10. Перечень помещений для обработки персональных данных;
11. Перечень информационных систем персональных данных;
12. Перечень применяемых средств защиты информации;
13. Технический паспорт информационных систем персональных данных;
14. Приказ о назначении лиц, ответственных за обработку и защиту персональных данных;
15. Инструкция администратора информационной безопасности;
16. Инструкция ответственного за обработку персональных данных;
17. Положение по обработке персональных данных;
18. Политика компании в отношении обработки персональных данных;
19. Положение об обеспечении безопасности персональных данных;
20. Регламент по определению уровней защищенности персональных данных в информационных системах;
21. Приказ об утверждении Инструкции пользователя информационных систем персональных данных;
22. Инструкция пользователя информационных систем персональных данных;
23. Регламент по учёту, хранению и уничтожению носителей персональных данных;
24. Регламент по допуску сотрудников и третьих лиц к обработке персональных данных;
25. Регламент по реагированию на запросы субъектов персональных данных;
26. Регламент по взаимодействию с органами государственной власти в области персональных данных;
27. Регламент по резервному копированию персональных данных;
28. Регламент по проведению контрольных мероприятий и реагированию на инциденты информационной безопасности;
29. Регламент по обезличиванию персональных данных;
30. Регламент по трансграничной передаче персональных данных.

**Стадия 4:ГАРАНТИЙНАЯ ПОДДЕРЖКА:**

Данный этап длится в течение года с момента заключения договора.

**Исполнитель обеспечивает:**

* Осуществление обновления и актуализации организационно-распорядительной документации по персональным данным
* Предоставление неограниченных консультаций, касающихся правоприменительной практики исполнения требований законодательства РФ по персональным данным и прохождения проверок Роскомнадзора в области персональных данных
* Предоставление финансовых гарантий в части компенсации штрафных санкций со стороны Роскомнадзора при проведении контрольно-надзорной деятельности в области персональных данных.

**ОСУЩЕСТВЛЕНИЕ ОБНОВЛЕНИЯ И АКТУАЛИЗАЦИИ ДОКУМЕНТОВ ПО ПЕРСОНАЛЬНЫМ ДАННЫМ:**

Осуществляется обновление и актуализация организационно-распорядительной документации по персональным данным. Основаниями для обновления и актуализации проектов документов по персональным данным являются изменения в законодательстве РФ по персональным данным, в судебной практике, в позиции регуляторов и результаты проведения контрольно-надзорных мероприятий Роскомнадзора в области персональных данных.

Изменения производятся ежеквартально с уведомлением ответственного лица со стороны Заказчика по e-mail и по телефону.

**ПРЕДОСТАВЛЕНИЕ НЕОГРАНИЧЕННЫХ КОНСУЛЬТАЦИЙ, КАСАЮЩИХСЯ ПРАВОПРИМЕНИТЕЛЬНОЙ ПРАКТИКИ ИСПОЛНЕНИЯ ТРЕБОВАНИЙ ЗАКОНОДАТЕЛЬСТВА РФ ПО ПЕРСОНАЛЬНЫМ ДАННЫМ И ПРОХОЖДЕНИЯ ПРОВЕРОК РОСКОМНАДЗОРА В ОБЛАСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ:**

Консультации оказываются по e-mail и средствами онлайн-чатов службой поддержки Исполнителя.

Обращения в службу поддержки обрабатываются в порядке их поступления. Реагирование на запрос осуществляется в течение 24 часов с момента поступления запроса. Если на этот период выпадает выходной или праздничный день, то срок предоставления ответа увеличивается на соответствующий период.

В случае, если для полного реагирования на запрос требуется срок, превышающий 24 часа, то специалист поддержки сообщает о необходимых сроках ответа на запрос не позднее 24 часов с момента поступления запроса, не считая выходные и праздничные дни.

**ПРЕДОСТАВЛЕНИЕ ФИНАНСОВЫХ ГАРАНТИЙ В ЧАСТИ КОМПЕНСАЦИИ ШТРАФНЫХ САНКЦИЙ СО СТОРОНЫ РОСКОМНАДЗОРА ПРИ ПРОВЕДЕНИИ КОНТРОЛЬНО-НАДЗОРНОЙ ДЕЯТЕЛЬНОСТИ В ОБЛАСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ:**

В случае, если в пределах сроков действия договора в отношении Заказчика проводятся контрольно-надзорные мероприятия со стороны Роскомнадзора, то специалисты Исполнителя консультируют сотрудников Заказчика по основным этапам проводимого контрольно-надзорного мероприятия и по необходимой информации для предоставления представителям Роскомнадзора.

В случае поступления от Роскомнадзора дополнительных вопросов в пределах сроков проведения контрольно-надзорного мероприятия специалисты Исполнителя консультируют по правильному ответу на него.

В случае выявления нарушений представителями Роскомнадзора время проведения контрольно-надзорного мероприятия, специалисты Исполнителя помогают их устранить в сроки проведения контрольно-надзорного мероприятия.

В случае получения от представителей Роскомнадзора предписания об устранении выявленных нарушений в области персональных данных, специалисты Исполнителя помогают и консультируют в части устранения нарушений в сроки, указанные в предписании.

В случае наложения на Заказчика штрафов по итогам контрольно-надзорного мероприятия Роскомнадзора в области персональных данных, Исполнитель компенсирует сумму таких штрафов в размере не превышающем стоимость договора.

**3. Сроки реализации проекта**

Стадии 1-3 - не более 50 рабочих дней с даты заключения договора

Стадия 1 – не более 35 рабочих дней

Стадия 2 – не более 5 рабочих дней

Стадия 3 – не более 10 рабочих дней

Стадия 4 - в течение года с даты заключения договора