Приложение № 2

к письму

**Перечень локальных актов по вопросам обработки персональных данных и защиты информации**

**I. ПРАВОВЫЕ МЕРЫ**

| **№ п/п** | **Документ** | **Нормативно-правовое обоснование** |
| --- | --- | --- |
| 1. | Типовые формы договоров, заключенных между оператором и субъектом персональных данных по основным направлениям деятельности оператора | Пункт 5 части 1 статьи 6 ФЗ № 152 |
| 2. | Копии договоров, заключенных с третьими лицами, касающихся передачи персональных данных, а также поручения на обработку персональных данных | Часть 3 статьи 6 ФЗ № 152  Статья 7 ФЗ № 152  Статья 88 Трудового кодекса РФ |
| 3. | Копии обращений от граждан (за два последних календарных года, включая текущий) по вопросам уточнения, удаления, уничтожения персональных данных, рассмотренные Оператором.  Копии ответов Оператора и принятые меры по обращениям граждан с приложением копий документов о принятых мерах | Статья 14 ФЗ № 152  Статья 89 Трудового кодекса РФ |
| 4. | Документы, подтверждающие согласие субъектов персональных данных (граждан и сотрудников оператора) на обработку/передачу их персональных данных (типовые формы) | Пункт 1 части 1 статьи 6 ФЗ № 152  Статьи 8, 10, 11, 12, 16 ФЗ № 152  Статья 88 Трудового кодекса РФ |
| 5. | Политика в отношении обработки персональных данных | Пункт 2 части 1 статьи 18.1 ФЗ № 152 |
| 5.1. | Скриншоты, подтверждающие размещение оператором в информационно-телекоммуникационной сети документа, определяющего его политику в отношении обработки персональных данных, и сведений о реализуемых требований к защите персональных данных  (в случае использования информационно-телекоммуникационной сети для сбора персональных данных) | Часть 2 статьи 18.1 ФЗ № 152 |
| 6. | Сведения об обработке персональных данных соискателей на замещение вакантных должностей:  - форма согласия соискателя на замещение вакантной должности на обработку персональных данных,  - сведения об обработке резюме, анкет соискателей (виды, сроки);  - сведения об использовании внешних сервисов (услуг) по подбору персонала, договоры с сервисами | Пункт 1 части 1 статьи 6 ФЗ № 152  Статья 86 Трудового кодекса РФ |
| 7. | Сведения о передаче персональных данных работников третьим лицам, в т.ч. поручения обработки персональных данных.  Рассмотрены могут быть направления (при наличии):  *аутсорсинг бухгалтерии, кадров;*  *зарплатный проект;*  *добровольное страхование (медицинское, от несчастных случаев и болезней);*  *медицинское обслуживание (диспансеризация, тестирование COVID-19);*  *корпоративная связь;*  *обучение;*  *транспорт (перевозки, доставка);*  *проживание;*  *подбор персонала;*  *обслуживание ИТ, информационных систем персональных данных;*  *внешние ИТ-сервисы (Office 365, Pruffme, Zoom, Google Workspace…);*  *иные услуги.*  По каждому направлению предоставляются:  договор с третьим лицом;  описание услуги, в т.ч. цели обработки персональных данных;  субъекты персональных данных;  согласие работника (в письменной форме, при необходимости);  согласие субъекта | Статья 86 Трудового кодекса Российской Федерации  Статья 7 ФЗ № 152  Статья 9 ч. 4 ФЗ № 152 |
| 8. | Справка о порядке оформления зарплатного проекта с приложением следующих документов:  Копия договора, заключенного с банком;  Копия документа отражающего основания передачи персональных данных работника банку с его согласия или без (копию договора на выпуск банковской карты для работника Оператора) | Пункт 3 статьи 86 Трудового кодекса Российской Федерации  Пункт 1 части 1 статьи 6 ФЗ № 152  Статья 9 ч. 4 ФЗ № 152 |
| 9. | Справка о порядке обработки персональных данных уволенных работников | Статья 14 ФЗ № 152  Пункт 4 статьи 21 №152-ФЗ |

**II. ОРГАНИЗАЦИОННЫЕ МЕРЫ**

| **№ п/п** | **Документ** | **Нормативно-правовое обоснование** |
| --- | --- | --- |
| 1. | Локальный акт о назначении ответственного за организацию обработки персональных данных (далее – персональных данных). Копия должностного регламента (должностные обязанности) или должностная инструкция ответственного за организацию обработки персональных данных | Пункт 2 части 1 статьи 18.1 ФЗ № 152 |
| 2. | **Локальные правовые акты по организации и обеспечению конфиденциальности и безопасности персональных данных граждан и сотрудников оператора при их обработке в т.ч. подтверждение ознакомления сотрудников с указанными актами, а также с положениями законодательства Российской Федерации о персональных данных в том числе:** | Пункт 2 части 1 статьи 18.1 ФЗ № 152 |
| 2.1. | положение по обработке персональных данных | Пункт 2 части 1 статьи 18.1 ФЗ № 152 |
| 2.2. | положение по обработке персональных данных работников | Статья 87 Трудового кодекса РФ |
| 2.3. | правила рассмотрения запросов субъектов персональных данных или их представителей | Части 1, 3 статьи 20 152-ФЗ  Статья 14 ФЗ № 152  ст. 88 Трудового кодекса РФ |
| 2.4. | правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора  Организован контроль за соответствием принимаемых мер по обеспечению безопасности персональных данных и установленного уровня защищенности персональных данных. Контроль проводится не реже 1 раза в 3 года (в том числе с привлечением лицензиатов ФСТЭК) | Пункт 4 части 1 статьи 18.1 ФЗ № 152  Часть 1 статьи 19 ФЗ № 152 |
| 2.5. | Перечни сотрудников, в должностные обязанности которых входит обработка персональных данных:  без использования средств автоматизации | Часть 1 статьи 18.1 ФЗ № 152  Пункты 13, 15 Постановления Правительства РФ от 15.09.2008 № 687 |
| 2.6. | с использованием средств автоматизации (пользователей информационных систем персональных данных);  с использованием СКЗИ (пользователей СКЗИ) | Часть 1 статьи 18.1 ФЗ № 152  Пункты 13-16 постановления Правительства Российской Федерации от 01.11.2012 № 1119  Пункты 5-8 приказа ФСБ России от 10.07.2014 № 378 |
| 2.7. | Сведения о фактах ознакомления с данными перечнями | Пункт 8 статьи 86 Трудового кодекса Российской Федерации  Пункт 6 части 1 статьи 18.1 ФЗ № 152  Пункт 6 Постановления Правительства РФ от 15.09.2008 № 687 |
| 3. | Документы, подтверждающие факты уничтожения персональных данных граждан и сотрудников оператора при достижении цели обработки персональных данных  акты уничтожения документов;  акты уничтожения персональных данных на носителях информации;  акты уничтожения персональных данных в информационных системах персональных данных;  либо справка подтверждающая, что уничтожения персональных данных не производилось (за три предыдущих года) | Пункт 6 статьи 5 ФЗ № 152,  Пункт 1 статьи 14 ФЗ № 152,  Пункт 2 части 1 статьи 18.1 ФЗ № 152  Часть 1 статьи 19 ФЗ № 152  Пункт 4 статьи 21 №152-ФЗ  ПП РФ № 687 |
| 4. | **Документы, принятые в рамках требований по неавтоматизированной обработке персональных данных** | Постановление Правительства РФ от 15.09.2008 № 687 |
| 4.1. | порядок обработки персональных данных на материальных носителях без использования средств автоматизации, в т.ч. хранение и уничтожение документов | Часть 3 статьи 5 ФЗ № 152;  Пункты 2, 3 части 1 статьи 18.1 ФЗ № 152;  Часть 1 статьи 19 ФЗ № 152 |
| 4.2. | приказ о назначении сотрудников, ответственных за хранение и уничтожение информации, содержащей персональные данные, документы, регламентирующие порядок хранения и уничтожения информации, содержащей персональные данные | Часть 3 статьи 5 ФЗ № 152;  Пункты 2, 3 части 1 статьи 18.1 ФЗ № 152;  Часть 1 статьи 19 ФЗ № 152;  Пункты 13-15 Постановления Правительства РФ от 15.09.2008 № 687 |
| 4.3. | утвержденный перечень мест хранения материальных носителей персональных данных (может быть на основе номенклатуры дел) | Пункты 13-15 Постановления Правительства РФ от 15.09.2008 № 687 |
| 4.4. | утвержденные формы документов (бланки), использующиеся при неавтоматизированной обработке персональных данных, содержащие поля, предназначенные для персональных данных сотрудников, граждан без содержания самих персональных данных (при наличии), а также связанные с ними документы, определяющие цели обработки ПД, имя, адрес оператора, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных:   * *согласия в письменной форме;* * *согласия на распространение персональных данных (при необходимости);* * *разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные.* * *запросы на уточнение, уничтожение, прекращение обработки персональных данных;* * *запросы сведений об обработке персональных данных в соответствии со статьей 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;* * *обязательства о неразглашении конфиденциальной информации, в том числе персональных данных;* * *журналы однократного пропуска на объект;* * *журнал учета обращений субъектов персональных данных;* * *анкеты, заявления, журналы и иные документы, предназначенные для сбора или учета в них сведений, содержащих персональные данные)* | Пункты 2,3 части 1 статьи 18.1 ФЗ № 152;  Часть 2 статьи 19 ФЗ № 152;  Статья 20 ФЗ № 152  Пункт 7 а) ПП РФ № 687 |
| 5. | **Документы, отражающие меры по ограничению физического доступа к персональным данным, а также меры охраны помещений и технических средств** |  |
| 5.1. | Приказ (положение) о пропускном и внутриобъектовом режиме в учреждении   * *журналы, реестры, книги, содержащие персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию оператора (при наличии);* * *журналы учета ключей, средств доступа (бесконтактные карты, брелоки), печатей для опечатывания* | Пункт 3 части 1 статьи 18.1 ФЗ № 152;  Пункт 13 постановления Правительства Российской Федерации от 01.11.2012 № 1119;  Пункт 15 Постановления Правительства РФ от 15.09.2008 № 687 |
| 5.2. | Приказы (положения, перечни) об ограничении доступа в помещения, в которых ведется обработка персональных данных | Статья 88 Трудового Кодекса РФ  Пункт 13 Постановления Правительства РФ от 15.09.2008 № 687 |
| 5.3. | Акт определения границ контролируемой зоны в учреждении | ЗТС.2 Приложение № 1 к Приказу ФСТЭК России от 18.02.2013 № 21 |
| 5.4. | Договор с охранной организацией на услуги охраны, включая приложения | Часть 1 статьи 6 ФЗ № 152;  Статья 7 ФЗ № 152;  Пункт 2 части 1 статьи 18.1 ФЗ № 152;  Часть 2 статьи 19 ФЗ № 152;  Статья 88 Трудового кодекса РФ |
| 5.5. | Договор на обслуживание средств охраны помещений | Часть 1 статьи 6 ФЗ № 152;  Статья 7 ФЗ № 152;  Пункт 2 части 1 статьи 18.1 ФЗ № 152;  Часть 2 статьи 19 ФЗ № 152;  Статья 88 Трудового кодекса РФ |
| 5.6. | Документы, отражающие проведение оператором оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом   * *порядок оценки возможного вреда;* * *акты (протоколы) оценки возможного вреда* | Пункт 5 части 1 статьи 18.1 ФЗ № 152 |
| 5.7. | Направления уведомления Роскомнадзора об обработке персональных для внесения организации в Реестр Операторов персональных данных (на сайте Роскомнадзора: https://pd.rkn.gov.ru/operators-registry/operators-list/)  Обеспечение актуализации сведений, содержащихся в уведомлении | Статья 22 ФЗ № 152 |

**III. МЕРЫ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ.**

**СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ (далее – СКЗИ)**

| **№ п/п** | **Документ** | **Нормативно-правовое обоснование** |
| --- | --- | --- |
| 1. | Перечень информационных систем, в которых производится обработка персональных данных, дать их описание и назначение, включая следующую информацию по каждой информационной системе:   * *адрес размещения базы данных информационной системы персональных данных, содержащих персональные данные граждан РФ;* * *категории субъектов персональных данных, обрабатываемых в информационных системах персональных данных;* * *категории персональных данных, обрабатываемых в информационных системах персональных данных (по каждой категории субъектов персональных данных), перечень действий с персональными данными, обрабатываемыми в информационной системе персональных данных;* * *инструкция к информационной системе персональных данных, руководство пользователя и любые аналогичные документы по функционалу информационных систем персональных данных, порядку доступа, резервирования;* * *описание технологического и информационного сопровождения информационных систем персональных данных;* * *скриншоты электронных шаблонов полей, содержащих персональные данные в информационных системах;* * *документы (договор аренды серверных мощностей, находящихся на территории Российской Федерации; документ, подтверждающий наличие у организации собственных серверных мощностей, на которых размещены базы персональных данных, подтверждающие размещение баз персональных данных на технических площадках (ЦОД, сервера), информационных системах, находящихся на территории Российской Федерации;* * *справка о постановке на балансовый учет ПЭВМ, на которых осуществляется обработка персональных данных* * *в случае сопровождения информационных систем персональных данных третьими лицами, необходимо приложить соответствующие договоры.* | Пункт 2 части 1 статьи 18.1 ФЗ № 152;  Часть 1 статьи 19 ФЗ № 152 |
| 2. | Документы, определяющие уровни защищенности персональных данных при их обработке в информационных системах персональных данных | Часть 1 статьи 19 ФЗ № 152;  Постановление Правительства Российской Федерации от 01.11.2012 № 1119 |
| 3. | Документ, отражающий определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных (частная модель угроз, утвержденный акт определения оценки угроз и т.п.) | Пункт 1 части 2 статьи 19 ФЗ № 152 |
| 4. | документ, определяющий меры безопасности персональных данных, которые необходимо принимать оператору для обеспечения установленного уровня защищенности персональных данных | Часть 1 статьи 19 ФЗ № 152;  Постановление Правительства Российской Федерации от 01.11.2012 № 1119  Приказ ФСТЭК России от 18.02.2013 № 21 |
| 5. | документ, отражающий проведение оценки эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных | Пункт 4 части 2 статьи 19 ФЗ № 152 |
| 6. | документы, подтверждающие применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации в организации | Пункт 3 части 2 статьи 19 ФЗ № 152 |
| 7. | Документы, регламентирующие процессы обеспечения безопасности персональных данных, обрабатываемых в информационных системах персональных данных:   * *инструкция пользователю по безопасной обработке персональных данных;* * *порядок обращения с машинными носителями информации;* * *инструкция по антивирусной защите в организации;* * *порядок предоставления доступа для сотрудников к информационным ресурсам оператора, содержащим персональные данные;* * *политика назначения и смены паролей в организации* * *правила безопасной работы в сети «Интернет» и с входящей электронной корреспонденцией;* * *инструкция по порядку учета, выдачи хранения, использования машинных носителей информации, обращения с ними, возврата и утилизации, а также уничтожения (стирания) информации на машинных носителях, в т.ч. порядок их передачи на техническое обслуживание.* * *инструкция о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации;* * *регламент реагирования на инциденты информационной безопасности* | Часть 1 статьи 19 ФЗ № 152;  Приказ ФСТЭК России от 18.02.2013 № 21 |
| 8. | Журналы в рамках эксплуатации информационных систем персональных данных:   * *Журнал учета съемных носителей конфиденциальной информации;* * *Журнал ознакомления сотрудников с локальными актами организации по вопросам обеспечения защиты информации (при необходимости, можно оформлять отдельные листы ознакомления на каждый локальный акт);* * *Журнал учета уничтожения носителей персональных данных и информации, содержащей персональные данные;* * *Журнал проведения инструктажей по информационной безопасности в организации;* * *Журнал учета проведения резервного копирования информации;* * *Журнал регистрации инцидентов информационной безопасности (событий безопасности)* | Пункт 2 части 1 статьи 18.1 ФЗ № 152;  Пункт 6 части 1 статьи 18.1 ФЗ № 152;  Пункт 5 части 2 статьи 19 ФЗ № 152;  Пункт 26 Приказа ФАПСИ от 13.06.2001 № 152  Приказ ФСТЭК России от 18.02.2013 № 21 |
| 9. | Копия приказа о назначении сотрудника, ответственного за безопасность персональных данных, администратора безопасности, системного администратора. Копия их должностных инструкций | Пункт 2 части 1 статьи 18.1 ФЗ № 152;  Пункты 16,17 Приказа ФСБ России от 10.07.2014 № 378 |
| 10. | Копии документов, регламентирующих порядок обмена персональными данными при их обработке в информационных системах (регламенты, инструкции) | Пункт 2 части 1 статьи 18.1 ФЗ № 152;  Часть 1 статьи 19 ФЗ № 152 |
| 11. | **Документы по эксплуатации СКЗИ** |  |
| 11.1. | Приказ о назначении ответственного за обеспечение безопасности хранения, обработки и передачи средств защиты информации в организации (либо администратора средств криптографической защиты информации), в случае использования для работы с информационными системами персональных данных СКЗИ | Пункты 16,17 Приказа ФСБ России от 10.07.2014 № 378;  Раздел V Приказа ФСБ РФ от 09.02.2005 № 66 |
| 11.2 | Приказ о назначении пользователей средств криптографической защиты информации, в случае использования для работы с информационными системами персональных данных СКЗИ | Пункт 19 Приказа ФАПСИ от 13.06.2001 № 152 |
| 11.3 | Приказ о назначении ответственного лица за учёт, выдачу ключей, печатей, пломбиров от помещений и сейфов в учреждении | Пункты 64,66 Приказа ФАПСИ от 13.06.2001 № 152 |
| 11.4 | Инструкция по обращению с сертифицированными шифровальными средствами (средствами криптографической защиты информации), инструкция пользователя средств криптографической защиты, инструкция ответственного за обеспечение безопасности хранения, обработки и передачи средств защиты информации (администратора средств криптографической защиты информации) | Пункт 2 части 1 статьи 18.1 ФЗ № 152;  Часть 1 статьи 19 ФЗ № 152;  Раздел V Приказа ФСБ РФ от 09.02.2005 № 66 |
| 11.5 | Наличие журналов:   * Журнал учета ключевых носителей; * Журнал поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов; * Журнал учёта ключей, печатей, пломбиров от помещений и сейфов; * Журнал контроля соблюдения условий эксплуатации и работоспособности средств криптографической защиты информации | Пункт 2 части 1 статьи 18.1 ФЗ № 152;  Часть 1 статьи 19 ФЗ № 152;  Приказ ФАПСИ от 13.06.2001 № 152 |

\_\_\_\_\_\_\_\_\_\_\_