Утверждено
Приказом генерального
директора Ассоциации
«Строители Волгоградского
региона»

№ 1 от «08» июня 2018г.

/И.П.ТОКАРЕВ/

ПОЛОЖЕНИЕ
ОБ ОБРАБОТКЕ И ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В
АССОЦИАЦИИ «СТРОИТЕЛИ ВОЛГОГРАДСКОГО РЕГИОНА»

г. Волгоград

СОДЕРЖАНИЕ

1 ОБЩИЕ ПОЛОЖЕНИЯ

Положение об обработке персональных данных, далее «Положение», в Ассоциации «Строители Волгоградского региона», далее Ассоциация «СВР», разработано в соответствии с:

– Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

– Постановлением Правительства Российской Федерации от 01.10.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Постановлением Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении положения в Ассоциации «Строители Волгоградского региона», далее Ассоциация «СВР», об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

– Приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

Настоящее Положение определяет порядок обработки персональных данных и устанавливает общие требования к обеспечению безопасности персональных данных, обрабатываемых в Ассоциации «СВР», как с использованием средств автоматизации, так и без использования таких средств.

Действие Положения распространяется на все структурные подразделения Ассоциации «СВР».

Настоящее Положение должно быть доведено до каждого работника Ассоциации «СВР», осуществляющего обработку персональных данных, под роспись в Листе ознакомления с настоящим Положением.

2 ОСНОВНЫЕ ПОНЯТИЯ

В Положении используются следующие основные понятия:

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Бумажный носитель персональных данных – материальный носитель графической и буквенно-цифровой информации, отраженной (зафиксированной) на бумаге.

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Инцидент - событие или группа событий, которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных.

Съемный носитель информации – сменный носитель данных, предназначенный для записи и считывания данных, представленных в стандартных кодах.

Обезличивание персональных данных - действия, в результате которых невозможно определить без использования дополнительной информации принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

3 ЦЕЛИ СБОРА И ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Ассоциацией «СВР» осуществляется обработка персональных данных следующей категории субъекта персональных данных:

– Физические лица, предоставляющие в Ассоциацию свои персональные данные для внесения этих данных в Национальный Реестр Специалистов НОСТРОЙ.

Настоящее положение разработано в целях:

- регламентации порядка осуществления операций с персональными данными физических лиц предоставляющих в Ассоциацию свои персональные данные (п. 1. настоящего Положения);
- обеспечения требований закона № 152-ФЗ «О персональных данных» и иных нормативно-правовых актов, регулирующих использование персональных данных;
- установления прав и обязанностей сотрудников Ассоциации в части работы с персональными данными;
- установления механизмов ответственности сотрудников предприятия за нарушение локальных норм, а также положений действующего законодательства РФ, регулирующего использование и хранение персональных данных.

Перечень субъектов персональных данных и обрабатываемых персональных данных приведен в таблице ниже (Таблица 1):

Таблица 1 – Перечень субъектов персональных данных и обрабатываемых персональных данных

№ п/п	Субъект ПДн	Перечень ПДн
1	физические лица	– паспорт или иной источник, удостоверяющий личность работника; – трудовая книжка; – свидетельство пенсионного страхования; – военный билет и иные документы воинского учета; – диплом об образовании; - ИНН;

4 ОРГАНИЗАЦИЯ ОБРАБОТКИ И ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1 Ответственные лица

Для организации работ по обработке и защите персональных данных в Ассоциации «СВР», приказом Генерального директора Токарева И. П. назначается Ответственный за организацию обработки персональных данных.

Для установления уровня защищенности персональных данных в информационной системе персональных данных, ввода системы защиты персональных данных в эксплуатацию, уничтожения персональных данных, а также расследования инцидентов безопасности персональных данных приказами Генерального директора могут назначаться специальные комиссии. В состав комиссий могут включаться руководители структурных подразделений, отвечающие

за отдельные направления работ по обеспечению обработки и безопасности персональных данных.

Для обеспечения защиты персональных данных при их автоматизированной обработке, приказом Генерального директора назначается Ответственный за обеспечение безопасности персональных данных при их обработке в информационной системе персональных данных (далее - Администратор информационной безопасности). Администратор информационной безопасности при обработке персональных данных в информационной системе обязан соблюдать условия настоящего положения, регламентирующие вопросы обработки и защиты персональных данных.

4.2 Порядок обработки персональных данных

Персональные данные субъекта персональных данных получаются от субъекта персональных данных (его представителя). В случае, если персональные данные получены не от субъекта персональных данных, Ассоциация «СВР» до начала обработки таких персональных данных обязана уведомить субъекта персональных данных о получении его персональных данных.

Систематизация, накопление хранение и использование персональных данных осуществляется путем оформления и ведения документов учета и баз данных, содержащих персональные данные. Работники Ассоциации «СВР», осуществляющие обработку персональных данных, должны обеспечить такую их обработку, чтобы она обеспечивала конфиденциальность персональных данных и исключала несанкционированный доступ к персональным данным третьих лиц.

Передача персональных данных субъектов персональных данных третьим лицам может осуществляться только при наличии письменного согласия субъекта персональных данных, если иное не предусмотрено Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных». Передача персональных данных субъектов персональных данных между подразделениями Ассоциации «СВР» должна осуществляться только между работниками, допущенными к обработке персональных данных.

Хранение персональных данных субъектов персональных данных осуществляется в информационной системе персональных данных, обеспечивающей сохранность персональных данных и их защиту от несанкционированного доступа.

В случае осуществления хранения персональных данных субъектов на бумажных носителях информации, такая информация подлежит уничтожению в течение тридцати дней с даты достижения цели обработки или срока обработки персональных данных. Уничтожение персональных данных на бумажных носителях информации производится комиссией, назначенной приказом Генерального директора, с обязательным составлением Акта о уничтожении материальных носителей персональных данных.

Ассоциация «СВР» уведомляет Уполномоченный орган по защите прав субъектов персональных данных (далее - Роскомнадзор) об обработке персональных данных. В случае изменения сведений, указанных в уведомлении, в случае прекращения обработки персональных данных, Ассоциация «СВР» также уведомляет об этом Роскомнадзор.

4.3 Допуск работников к обработке персональных данных

Допуск работников Ассоциации «СВР» к обработке персональных данных осуществляется на основании приказа о назначении на должность в соответствии с Перечнем работников и подразделений Ассоциации «СВР», допущенных к обработке персональных данных для выполнения ими служебных (трудовых) обязанностей, после выполнения следующих мероприятий:

– ознакомления под роспись с руководящими документами Ассоциации «СВР» по обработке и защите персональных данных;

– оформления письменного обязательства о неразглашении сведений конфиденциального характера.

Работники Ассоциации «СВР», обрабатывающие персональные данные, имеют право обрабатывать только те персональные данные, которые им необходимы для выполнения служебных (трудовых) обязанностей.

4.4 Обязанности работника при обработке персональных данных

Работник при работе с персональными данными, обязан:

– соблюдать режим конфиденциальности персональных данных;

– выполнять требования инструкций, регламентирующим процессы обработки и защиты персональных данных;

– передавать персональные данные только тем работникам, которые допущены к их обработке;

– обеспечивать надежное хранение носителей персональных данных;

– своевременно сообщать непосредственному руководителю о ставших известными попытках посторонних лиц получить доступ к защищаемым персональным данным;

– немедленно уведомлять непосредственного руководителя и принимать меры по предотвращению утечки персональных данных при выявлении фактов утраты или недостачи ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений;

– сдать носители персональных данных (при наличии) в соответствии с порядком, установленным настоящим Положением, при увольнении или отстранении от исполнения обязанностей, связанных с обработкой персональных данных

Работнику, осуществляющему обработку персональных данных, запрещается:

– записывать на учтенные машинные носители (при наличии) информацию, не имеющую отношения к выполняемой работе;

– принимать и передавать носители персональных данных без соответствующего разрешения и оформления в установленном порядке;

– хранить носители персональных данных на рабочих столах либо оставлять их без присмотра

Ответственные лица должны пресекать действия работников и других лиц, которые могут привести к хищению или разрушению носителей персональных данных, и сообщать о фактах таких действий вышестоящему руководству.

4.5 Предоставление персональных данных на обработку третьей стороне

Персональные данные могут быть переданы на обработку третьей стороне только при наличии согласия субъекта персональных данных на передачу персональных данных субъекта персональных данных третьей стороне.

4.6 Требования к системе защиты персональных данных

Безопасность персональных данных при их обработке в информационной системе персональных данных обеспечивается с помощью системы защиты, реализованной организационными и техническими мерами.

Система защиты персональных данных Ассоциации «СВР» обеспечивает:

– нейтрализацию актуальных угроз безопасности персональных данных;

– проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к персональным данным;

– своевременное обнаружение фактов несанкционированного доступа к персональным данным;

– недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

– возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– постоянный контроль обеспечения уровня защищенности персональных данных

В информационной системе персональных данных Ассоциации «СВР» используются средства защиты информации, прошедшие в установленном порядке процедуру оценки соответствия требованиям по безопасности информации.

Общий контроль соблюдения требований по защите персональных данных осуществляет Ответственный за организацию обработки персональных данных.

Контроль соблюдения порядка и условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией, возлагается на Администратора информационной безопасности.

Работники Ассоциации «СВР», использующие средства защиты информации для обеспечения безопасности персональных данных, должны быть обучены правилам работы с ними.

Разработка и проведение мероприятий по обеспечению безопасности персональных данных, обрабатываемых в информационной системе персональных данных Ассоциации «СВР», осуществляется силами и средствами Ассоциации «СВР», либо на договорной основе сторонней организацией, имеющей лицензию на деятельность по технической защите конфиденциальной информации.

4.7 Порядок создания системы защиты персональных данных

Для создания (модернизации) системы защиты персональных данных проводятся следующие мероприятия и работы:

- обследование порядка обработки персональных данных в информационной системе персональных данных;
- определение угроз и нарушителя безопасности персональных данных при их обработке в информационной системе персональных данных;
- установление уровня защищенности персональных данных;
- определение состава и содержания мер по обеспечению безопасности персональных данных;
- проектирование системы защиты персональных данных;
- закупка и внедрение средств защиты информации;
- ввод системы защиты персональных данных в эксплуатацию.

4.7.1 Обследование обработки персональных данных в информационной системе персональных данных

Обследование обработки персональных данных в информационной системе персональных данных проводится с целью определения (актуализации) состава, структуры информационной системы персональных данных принятых мер безопасности, содержания и объема обрабатываемых персональных данных, а также взаимодействия информационной системы персональных данных с иными системами и телекоммуникационными сетями общего пользования. На основании обследования вырабатываются рекомендации по совершенствованию существующей системы защиты персональных данных.

4.7.2 Определение угроз безопасности

Актуальные угрозы безопасности персональных данных при их обработке в информационной системе персональных данных определяются исходя из наличия вероятного нарушителя, возможных способов и средств реализации угроз. На их

основе в соответствии с методическими документами ФСТЭК и ФСБ России формируются Модель угроз и Модель нарушителя безопасности персональных данных.

4.7.3 Установление уровня защищенности персональных данных

Для персональных данных в соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» с учетом актуальных угроз безопасности, специально назначенной комиссией устанавливается уровень защищенности персональных данных. Результаты установления уровня защищенности персональных данных при их обработке в информационной системе персональных данных Ассоциации «СВР» оформляются Актами.

4.7.4 Определение состава и содержания мер по обеспечению безопасности персональных данных

Выбор мер по защите персональных данных в информационной системе персональных данных осуществляется на основе уровня ее защищенности с учетом структуры информационной системы персональных данных, применяемых технических средств и информационных технологий, а также актуальных угроз безопасности персональных данных.

Система защиты персональных данных в соответствии с требованиями:

– Приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Приказа ФСБ России от 10.07.2014 № 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»;

реализована следующими группами мер:

– идентификация и аутентификация субъектов доступа и объектов доступа;
– управление доступом субъектов доступа к объектам доступа;
– ограничение программной среды;
– защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные;
– регистрация событий безопасности;
– антивирусная защита;
– обнаружение (предотвращение) вторжений;

– контроль (анализ) защищенности персональных данных;

– обеспечение целостности информационной системы персональных данных и персональных данных;

– обеспечение доступности персональных данных;

– защита среды виртуализации;

– защита технических средств;

– защита информационной системы персональных данных, ее средств, систем связи и передачи данных;

– выявление инцидентов и реагирование на них;

– управление конфигурацией информационной системы персональных данных и системы защиты персональных данных.

Состав и содержание мер защиты персональных данных, необходимых для реализации в информационной системе персональных данных отражены в техническом задании на создание системы защиты персональных данных.

4.7.5 Проектирование системы защиты персональных данных

Проектирование системы защиты заключается в выработке вариантов технических решений по реализации установленных мер обеспечения безопасности персональных данных с учетом существующих способов и средств защиты информации.

По результатам проектирования оформляется технический проект системы защиты.

4.7.6 Закупка и внедрение средств защиты

Закупка средств защиты информации в соответствии с техническим проектом осуществляется за счет бюджета Ассоциации «СВР».

Все работы по установке, монтажу и испытанию средств защиты информации производятся Ассоциации «СВР» самостоятельно либо сторонней организацией, имеющей лицензию на деятельность по технической защите конфиденциальной информации.

В процессе пуско-наладочных работ средства защиты информации устанавливаются, настраиваются и испытываются на готовность к использованию в информационной системе персональных данных Ассоциации «СВР». При положительных результатах средства защиты вводятся в эксплуатацию с составлением Акта. Установка, проверка и ввод средств защиты информации в эксплуатацию производится в соответствии с эксплуатационной и технической документацией на эти средства защиты комиссией организации – исполнителя работ.

4.7.7 Ввод системы защиты в эксплуатацию

На основании решения Генерального директора Ассоциации «СВР» издается приказ о вводе системы защиты в эксплуатацию.

4.8 Организационные меры защиты

Для обеспечения безопасности персональных данных при их обработке в информационной системе персональных данных Ассоциации «СВР», применяются следующие организационные меры:

- сертифицированный ФСТЭК России антивирус ESET NOD32 Secure Enterprise Pack 5.0.
- межсетевой экран Traffic Inspector FSTEC, сертифицированное ФСТЭК России.

5 ОСОБЕННОСТИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

В случае обработки персональных данных физических лиц, предоставляющих в Ассоциацию «СВР» свои персональные данные для внесения этих данных в Национальный Реестр Специалистов НОСТРОЙ - без использования средств автоматизации, должны соблюдаться следующие требования:

Обработка персональных данных субъектов персональных данных без использования средств автоматизации осуществляется в виде документации на бумажных носителях (доступ к которым также осуществляется в соответствии с положениями локальных правовых актов и законодательства РФ). Персональные данные при их обработке без использования средств автоматизации обособляются от иной информации путем фиксации их на отдельных материальных (бумажных) носителях персональных данных.

При фиксации персональных данных на материальных носителях не допускается запись на одном материальном носителе персональных данных, цели обработки которых заведомо несовместимы. При обработке различных категорий персональных данных без использования средств автоматизации, для каждой категории персональных данных используется отдельный материальный носитель.

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, соблюдаются следующие условия:

– типовая форма содержит сведения о цели обработки персональных данных, наименование и адрес Ассоциации «СВР», фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых Ассоциации «СВР» способов обработки персональных данных;

– типовая форма предусматривает поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных;

– типовая форма составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

– типовая форма исключает объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных.

Обеспечивается раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе.

Уточнение персональных данных при их обработке без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя – путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

Лица, осуществляющие обработку персональных данных без использования средств автоматизации, проинформированы:

– о факте обработки ими персональных данных, обработка которых осуществляется без использования средств автоматизации;

– о категориях обрабатываемых персональных данных;

– об особенностях и правилах осуществления такой обработки.

6 ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ

В целях осуществления внутреннего контроля соответствия обработки персональных данных работниками Ассоциации «СВР», осуществляющими обработку персональных данных в информационной системе персональных данных Ассоциации «СВР», могут организовываться периодические проверки условий обработки персональных данных.

Проверки организуются и осуществляются Ответственным за организацию обработки персональных данных или специально назначенной комиссией.

По результатам проверки с целью информирования руководства Ассоциации «СВР» составляется Акт с указанием выявленных недостатков и предложений по их устранению.

Перечень мероприятий по контролю, его периодичность, а также ответственные лица устанавливаются Планом мероприятий по обеспечению информационной безопасности в Ассоциации «СВР».

Для проведения внешнего контроля и аудита обработки персональных данных Ассоциации «СВР» на договорной основе может привлекаться сторонняя организация, имеющая лицензию на деятельность по технической защите конфиденциальной информации

7 ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Иные права и обязанности работников, в служебные обязанности которых входит обработка персональных данных, определяются их должностными инструкциями.

Работники Ассоциации «СВР», виновные в нарушении требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», несут предусмотренную законодательством Российской Федерации ответственность.