



Inspired by patients.
Driven by science.

Утверждено Приказом Генерального директора № 23
от 12 апреля 2021 года

Подпись _____

Булычев Павел Юрьевич

Генеральный директор

М.П.



ПОЛОЖЕНИЕ

ОБ ОРГАНИЗАЦИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБЩЕСТВЕ С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "ЮСБ ФАРМА"

г. Москва, 2021

Приложение 1
к Приказу Генерального директора
Общества с ограниченной ответственностью "ЮСБ Фарма"
№ 23 от 12 апреля 2021 года

**ПОЛОЖЕНИЕ ОБ ОРГАНИЗАЦИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В
ОБЩЕСТВЕ С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "ЮСБ ФАРМА"**

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. В настоящем *Положении об организации обработки персональных данных в Обществе с ограниченной ответственностью "ЮСБ Фарма" ("Положение")* определен порядок обработки персональных данных ("ПДн"), меры, направленные на защиту ПДн, а также процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в области ПДн в Обществе с ограниченной ответственностью "ЮСБ Фарма" (далее – "Общество" или "Оператор").

1.2. Настоящее Положение разработано в целях:

- организации обработки ПДн работников Общества и иных Субъектов ПДн, осуществляющей Обществом как оператором ПДн, а также в случаях, когда обработка ПДн поручена Обществу другим оператором ПДн в соответствии с требованиями действующего законодательства Российской Федерации;
- обеспечения защиты прав и свобод человека и гражданина при обработке его ПДн, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.3. Настоящее Положение разработано с учетом следующих нормативно-правовых актов:

- Конституция Российской Федерации;
- Трудовой кодекс Российской Федерации;
- Гражданский кодекс Российской Федерации;
- Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации";
- Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных" ("Закон о персональных данных");
- Постановление Правительства Российской Федерации от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";
- Постановление Правительства Российской Федерации от 15.09.2008 № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляющей без использования средств автоматизации";
- иные нормативно-правовые акты Российской Федерации, регламентирующие вопросы обработки ПДн.

1.4. В части, не урегулированной настоящим Положением, применяются нормы действующего законодательства Российской Федерации.

1.5. Все работники Общества должны быть ознакомлены с настоящим Положением и любыми изменениями к нему под подпись и должны руководствоваться в своей деятельности настоящим

Положением и принятыми в соответствии с ним локальными нормативными актами. Информация об ознакомлении работников фиксируется в *Журнале учета ознакомления с правилами обработки персональных данных*, форма которого приведена в Приложении 1 к настоящему Положению.

1.6. Особенности обработки ПДн, собранных посредством ресурсов Общества (веб-сайт <https://www.ucbrussia.ru/>, контактные телефонные номера Общества, адреса электронной почты Общества), регулируются Политикой в отношении обработки персональных данных, опубликованной на веб-сайте Общества <https://www.ucbrussia.ru/>.

2. ОСНОВНЫЕ ТЕРМИНЫ И СОКРАЩЕНИЯ

2.1. Следующие употребляемые в настоящем Положении термины имеют указанные ниже значения:

- "**Автоматизированная обработка персональных данных**" – обработка персональных данных с помощью средств вычислительной техники.
- "**Биометрические персональные данные**" – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности Субъекта ПДн.
- "**Блокирование персональных данных**" – временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн).
- "**Доступность ПДн**" – состояние ПДн (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.
- "**Контрагент**" – физическое лицо, индивидуальный предприниматель, работники и представители контрагентов, подписанты договоров, действующие как в собственных интересах, так и представляющих интересы третьих лиц в их отношениях с Обществом в рамках или в связи с предполагаемыми/заключаемыми или заключенными гражданско-правовыми договорами.
- "**Конфиденциальность персональных данных**" – обязанность оператора и иных лиц, получивших доступ к ПДн, не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено законодательством Российской Федерации.
- "**Материальный носитель**" – машиночитаемый носитель информации (в том числе магнитный и электронный), на котором осуществляются запись и хранение ПДн, а также содержащие ПДн документы.
- "**Неавтоматизированная обработка персональных данных**" – обработка ПДн без использования средств автоматизации (без помощи средств вычислительной техники).
- "**Обработка**" означает любое действие (операцию) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.
- "**Оператор**" – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн.

- "Оценка возможного вреда" – определение уровня вреда на основании учёта возможных убытков и морального вреда, нарушения конфиденциальности, целостности и доступности ПДн.
- "Персональные данные" или "ПДн" – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу.
- "Персональные данные, разрешенные субъектом персональных данных для распространения" – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Законом о персональных данных.
- "Работник" означает физическое лицо, вступившее в трудовые отношения с Обществом.
- "Распространение персональных данных" – действия, направленные на раскрытие ПДн неопределенному кругу лиц.
- "Субъекты", "Субъекты ПДн" означает Работников, Бывших Работников, Родственников Работников, Соискателей на вакантную должность, Работников контрагентов и потенциальных контрагентов (работников организаций – поставщиков товаров, работ, услуг, бизнес-партнеров), а также физических лиц и индивидуальных предпринимателей – поставщиков товаров, работ, услуг, бизнес-партнеров, Специалистов здравоохранения, Пользователей, Посетителей офиса, Работников иных компаний группы ЮСБ в России, Контрагентов иных компаний группы ЮСБ в России, иных лиц, чьи ПДн обрабатываются Обществом.
- "Трансграничная передача персональных данных" – передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.
- "Уничтожение ПДн" – действия, в результате которых становится невозможным восстановить содержание ПДн в информационной системе ПДн и (или) в результате которых уничтожаются материальные носители ПДн.
- "Целостность ПДн" – состояние ПДн, при котором отсутствует любое их изменение либо изменение осуществляется только преднамеренно субъектами, имеющими право на такое изменение.

3. ОБЩИЕ УСЛОВИЯ И ПОРЯДОК ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБЩЕСТВЕ

3.1. Обработка ПДн в Обществе может осуществляться исключительно при наличии одного из следующих правовых оснований:

- обработка ПДн осуществляется с согласия Субъекта ПДн на обработку его ПДн;
- обработка ПДн необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на Общество функций, полномочий и обязанностей;
- обработка ПДн необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;
- обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является Субъект ПДн, а также для заключения договора по инициативе Субъекта ПДн или договора, по которому Субъект ПДн будет являться выгодоприобретателем или поручителем;

- обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов Субъекта ПДн, если получение согласия Субъекта ПДн невозможно;
- обработка ПДн необходима для осуществления прав и законных интересов оператора или третьих лиц, либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПДн;
- обработка ПДн осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 Закона о персональных данных, при условии обязательного обезличивания ПДн;
- осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законодательством Российской Федерации.

3.2. Общество обрабатывает ПДн субъектов следующих категорий: Работников, Бывших Работников, Родственников Работников, Соискателей на вакантную должность, Работников контрагентов и потенциальных контрагентов (работников организаций – поставщиков товаров, работ, услуг, бизнес-партнеров), а также физических лиц и индивидуальных предпринимателей – поставщиков товаров, работ, услуг, бизнес-партнеров, Специалистов здравоохранения, Пользователей, Посетителей офиса, Работников иных компаний группы ЮСБ в России, Контрагентов иных компаний группы ЮСБ в России, иных лиц, чьи ПДн обрабатываются Обществом.

3.3. Категории обрабатываемых Обществом ПДн, цели обработки ПДн, сроки обработки и условия прекращения обработки ПДн определяются Генеральным директором Общества и (или) лицом, ответственным за организацию обработки ПДн, и закрепляются в *Перечне персональных данных*.

3.4. *Перечень персональных данных* формируется лицом, ответственным за организацию обработки ПДн в Обществе, с учетом текущих потребностей и бизнес-процессов Общества, и утверждается Приложением к настоящему Положению. Обработка ПДн, которые не были включены в *Перечень персональных данных*, не допускается, за исключением случаев, когда обязанность осуществлять такую обработку предусмотрена действующим законодательством.

3.5. Общество не обрабатывает специальные категории ПДн, касающихся расовой и национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни, кроме случаев, когда обработка ПДн о состоянии здоровья осуществляется в соответствии с трудовым законодательством, с законодательством о государственной социальной помощи, законодательством об обязательном социальном страховании на случай временной нетрудоспособности и в связи с материнством, пенсионным законодательством Российской Федерации, а также иных случаев, когда такая обработка необходима для определенных целей и ведется при наличии законных оснований (например, письменное согласие субъекта ПДн).

3.6. Общество не обрабатывает биометрические ПДн.

3.7. Общество не принимает решений, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы, на основании исключительно автоматизированной обработки его ПДн.

3.8. В случае возникновения необходимости получения ПДн у третьих лиц, следует до начала обработки известить Субъекта ПДн об этом, сообщив ему о наименовании и адресе оператора, целях и правовых основаниях, предполагаемых пользователях ПДн, источниках и способах получения ПДн, а также о предусмотренных Законом о персональных данных правах субъекта ПДн. Общество вправе не извещать Субъекта ПДн об обработке полученных у третьих лиц ПДн, если субъект был уведомлен об осуществлении обработки соответствующим оператором, либо если обработка ПДн, разрешенных Субъектом ПДн для распространения, осуществляется с

соблюдением запретов и условий, предусмотренных ст. 10.1. Закона о персональных данных, а также в иных случаях, предусмотренных Законом о персональных данных.

3.9. В целях организации информационного обеспечения и коммуникаций Общество может, в случае необходимости, создавать и вести внутренние справочники Оператора, доступ к которым имеет ограниченный круг лиц, принявших на себя обязательства по обеспечению конфиденциальности соответствующих ПДн. Указанные внутренние справочники создаются, в том числе, с использованием собственных информационных систем ПДн Оператора и информационных систем ПДн, владельцами которых являются иные лица.

3.10. При сборе ПДн Субъектов ПДн, являющихся гражданами Российской Федерации, Общество обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение ПДн с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в Законе о персональных данных.

3.11. *Перечень мест хранения документов, содержащих персональные данные*, утверждается Приложением к настоящему Положению. В случае необходимости внесения изменений в *Перечень мест хранения документов, содержащих персональные данные*, заинтересованное лицо обязано обратиться к лицу, ответственному за организацию обработки ПДн в Обществе, с целью внесения изменений в *Перечень мест хранения документов, содержащих персональные данные*. Хранение документов, содержащих ПДн, в помещениях или иных местах хранения, не включенных в *Перечень мест хранения документов, содержащих персональные данные*, не допускается.

3.12. С учетом особенностей и в части, не противоречащей действующему законодательству и настоящему Положению, обработка ПДн в Обществе также должна осуществляться с соблюдением принципов, предусмотренных глобальными политиками группы компаний UCB.

4. ПРАВИЛА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

4.1. Для каждого процесса неавтоматизированной обработки должна быть определена цель обработки, которая должна быть указана в *Перечне персональных данных*.

4.2. ПДн при неавтоматизированной обработке должны обособляться от иной информации, в частности путем фиксации их в отдельных документах, в специальных разделах или на полях форм (бланков).

4.3. Неавтоматизированная обработка ПДн должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения ПДн, предназначенные для обработки ПДн без использования средств автоматизации, и установить перечень лиц, осуществляющих обработку ПДн, которые должны быть приведены в *Перечне мест хранения документов, содержащих персональные данные*.

4.4. При хранении документов, содержащих ПДн, должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный доступ к ним.

4.5. Лица, осуществляющие неавтоматизированную обработку ПДн (в том числе лица, допущенные к обработке ПДн, и лица, осуществляющие такую обработку по поручению оператора), должны быть проинформированы о факте обработки ими ПДн, категориях обрабатываемых ПДн, а также об особенностях и правилах осуществления обработки ПДн, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными нормативными актами Общества.

4.6. Общество должно обеспечивать раздельное хранение ПДн, обработка которых осуществляется в различных целях. При фиксации в документах, содержащих ПДн, не допускается фиксация в одном документе ПДн, цели обработки которых заведомо несовместимы.



4.7. При ведении журналов (реестров, книг), содержащих ПДн, необходимых для однократного пропуска субъекта ПДн на территорию, на которой находится оператор, или в иных аналогичных целях, должны соблюдаться следующие условия:

- необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена локальным нормативным актом Общества, содержащим сведения о цели обработки ПДн, осуществляющей без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов ПДн, перечень лиц (поименно или по должностям), имеющих доступ к документам, содержащим ПДн и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки ПДн, а также сведения о порядке пропуска субъекта ПДн на территорию, на которой находится оператор, без подтверждения подлинности ПДн, сообщенных субъектом ПДн;
- копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;
- ПДн каждого субъекта ПДн могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта ПДн на территорию, на которой находится оператор.

4.8. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн (далее – **"Типовая форма"**), должны соблюдаться следующие условия:

- Типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки ПДн, осуществляющей без использования средств автоматизации, наименование и адрес Общества, фамилию, имя, отчество и адрес субъекта ПДн, источник получения ПДн, сроки обработки ПДн, перечень действий с ПДн, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки ПДн;
- Типовая форма должна предусматривать поле, в котором субъект ПДн может поставить отметку о своем согласии на обработку ПДн, осуществляющую без использования средств автоматизации – при необходимости получения письменного согласия на обработку ПДн;
- Типовая форма должна быть составлена таким образом, чтобы каждый из субъектов ПДн имел возможность ознакомиться со своими ПДн, содержащимися в документе, не нарушая прав и законных интересов иных субъектов ПДн;
- Типовая форма должна исключать объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.

4.9. Уточнение ПДн при осуществлении неавтоматизированной обработки ПДн производится путем обновления или изменения данных в документах, содержащих ПДн, путем фиксации на том же документе сведений о вносимых в них изменениях, либо путем изготовления нового документа с уточненными ПДн.

4.10. За нарушение правил обработки ПДн, их неправомерное разглашение или распространение, виновные ответственные работники несут дисциплинарную, материальную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством.

5. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

5.1. Право доступа к ПДн имеют:

- руководство Общества – ко всем ПДн с целью обеспечения эффективного управления и руководства деятельностью Общества;

- Работники Общества – к тем данным, которые необходимы им для выполнения должностных обязанностей и обеспечения эффективной деятельности Общества;
- Работники организации, оказывающей Обществу услуги по ведению кадрового делопроизводства и бухгалтерские услуги на основании соответствующего договора – к тем данным, которые необходимы им для исполнения соответствующего договора;
- Работники иных компаний группы ЮСБ в России – к тем данным, которые необходимы им в рамках осуществления деятельности компаний группы ЮСБ в России;
- сам Субъект ПДн – к своим собственным ПДн в соответствии с действующим законодательством.

5.2. Лица, получающие ПДн, обязаны использовать ПДн лишь в тех целях, для которых они сообщены. Любые лица, получающие ПДн, обязаны соблюдать режим секретности (конфиденциальности). Работники обязаны не разглашать ПДн Субъектов ПДн и иных лиц.

6. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. В случаях, предусмотренных Законом о персональных данных, Общество может осуществлять передачу ПДн государственным и муниципальным органам и иным операторам ПДн. В частности, Общество может передавать ПДн следующим органам власти:

- налоговые органы;
- финансовые органы;
- правоохранительные органы;
- миграционные органы;
- органы исполнительной власти, уполномоченные в области противодействия техническим разведкам и технической защиты информации;
- органы исполнительной власти, уполномоченные в области безопасности;
- органы, осуществляющие функции по контролю и надзору в сфере связи, информационных технологий и массовых коммуникаций;
- антимонопольные органы;
- органы исполнительной власти, осуществляющие официальный статистический учет и контроль в сфере официального статистического учета;
- органы, осуществляющие государственный надзор за соблюдением трудового законодательства;
- военные комиссариаты и иные органы, осуществляющие воинский учет;
- органы социальной защиты;
- органы социального страхования;
- пенсионные фонды;
- органы, осуществляющие функции по контролю и надзору в сфере здравоохранения;
- подразделения муниципальных органов управления.

6.2. Передача ПДн для обработки иным третьим лицам в иных случаях допускается при одновременном соблюдении условий, указанных ниже:

- обработка третьим лицом ПДн, предоставленных Обществу Субъектом ПДн (его законным представителем), может осуществляться только в следующих случаях:
 - с согласия субъекта ПДн (его законного представителя), если получение такого согласия необходимо в соответствии с требованиями Закона о персональных данных; или
 - обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем или поручителем; или
 - если третье лицо, которому передаются ПДн, подтвердит наличие у него иных законных оснований для получения ПДн у Общества и его последующей обработки.
- кроме случаев, когда законодательством допускается иное, передача ПДн третьему лицу может осуществляться только на основании договора, заключенного с Обществом, в котором:
 - установлена обязанность третьего лица соблюдать конфиденциальность ПДн и обеспечивать безопасность ПДн при их обработке;
 - установлена обязанность третьего лица не раскрывать и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено законодательством Российской Федерации;
 - в случае поручения Обществом третьему лицу осуществлять обработку ПДн в таком договоре определены перечень действий (операций), которые будут осуществляться с ПДн, цели обработки ПДн, а также указаны требования к защите обрабатываемых ПДн в соответствии со статьей 19 Закона о персональных данных.

6.3. Общество может осуществлять трансграничную передачу ПДн только при условии, что при сборе передаваемых ПДн была обеспечена запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение ПДн граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в Законе о персональных данных. Общество может осуществлять трансграничную передачу ПДн на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов ПДн, только в случаях, предусмотренных статьей 12 Закона о персональных данных.

6.4. Ответы на письменные запросы государственных органов и третьих лиц даются в письменной форме на бланке Общества и в том объеме, который позволяет не разглашать избыточный объем ПДн о субъектах ПДн.

7. ОСОБЕННОСТИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ

7.1. Работники и их представители должны быть ознакомлены под роспись с документами Общества, устанавливающими порядок обработки ПДн Работников, а также об их правах и обязанностях в этой области.

7.2. При оформлении трудовых отношений с Работником формируется личная папка Работника. Личные папки хранятся в бумажном виде. Личные дела находятся в специально отведенных

металлических архивных шкафах, обеспечивающих защиту от несанкционированного доступа. Ответственным за ведение и хранение/обеспечение надлежащего хранения личных дел Работников является Директор по управлению персоналом и финансовыми услугами России, и международными рынками Общества.



7.3. Личная папка Работника состоит из следующих документов:

- трудовой договор;
- документы, связанные с трудовой деятельностью (аттестационные листы, документы, связанные с переводом, дополнительные соглашения к трудовому договору, должностные инструкции, рекомендации, характеристики, резюме, др.);
- Распоряжение о назначении выгодоприобретателя, заявление на перечисление заработной платы, приказ о приеме на работу, справки 2-НДФЛ и 182-н с предыдущего места работы или за последние 2 года, военный билет (при наличии), иные документы, связанные с трудовой деятельностью.

7.4. Личная карточка Работника – документ унифицированной формы № Т-2, который заполняется на основании приказа (распоряжения) о приеме на работу на Работников всех категорий. Личная карточка работника ведется на протяжении всей трудовой деятельности Работника. Изменения, вносимые Обществом, должны быть подтверждены соответствующими документами.

7.5. Общество, кроме личных дел, создает и хранит / обеспечивает хранение следующих документов, содержащих ПДн Работников:

- трудовые книжки;
- карточки Т-2;
- подлинники и копии приказов (распоряжений) по кадрам;
- материалы аттестаций и повышения квалификаций работников;
- материалы внутренних расследований (акты, докладные, протоколы и др.);
- копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения;
- другие.

7.6. Трудовые книжки Работников хранятся в пожаростойком сейфе.

7.7. Кадровые приказы, табели учета рабочего времени, журналы регистрации, иные документы, содержащие ПДн Работников, хранятся в специальных папках в запираемых ящиках картотеки. Также ПДн Работников хранятся в отделе персонала в электронном виде.

7.8. Работники не должны отказываться от своих прав на сохранение и защиту тайны.

7.9. Если в соответствии с действующим законодательством для обработки ПДн Работника требуется его письменное согласие, то Общество имеет право обрабатывать такие ПДн Работника только после получения его письменного согласия.

7.10. Все ПДн Работника следует получать у него самого. Если ПДн возможно получить только у третьей стороны, то Работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Общество должно сообщить Работнику о целях, предполагаемых источниках и способах получения ПДн, а также о характере подлежащих получению ПДн и последствиях отказа Работника дать письменное согласие на их получение.

7.11. Общество имеет право получать и обрабатывать ПДн Работника о его членстве в общественных объединениях или его профсоюзной деятельности только в случаях, предусмотренных законодательством Российской Федерации.

7.12. При принятии решений, затрагивающих интересы Работника, Общество не имеет права основываться на ПДн, полученных исключительно в результате их автоматизированной обработки или электронного получения.



7.13. Защита ПДн Работника от неправомерного их использования или утраты должна быть обеспечена Обществом за счет собственных средств в порядке, установленном законодательством Российской Федерации.

7.14. Работник обязан использовать оборудование или средства связи, принадлежащие или оплачиваемые Обществом, исключительно в целях, предусмотренных локальными нормативными актами Общества. Общество имеет право в любое время извлекать, просматривать и читать любые файлы, документы или сообщения, созданные, отправленные или полученные Работниками с использованием оборудования или средств связи, принадлежащих или оплачиваемых Обществом (которые в этой связи считаются служебными файлами, документами и сообщениями), без дальнейшего уведомления. Общество также вправе обрабатывать сведения о Работниках, полученные посредством систем видеонаблюдения, применяемых в Обществе, в отношении вопросов обеспечения соблюдения законов и иных нормативных правовых актов, обеспечения личной безопасности Работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества, соблюдения локальных нормативных актов Обществе.

7.15. В целях обеспечения защиты ПДн, которые хранит / обеспечивает хранение Общество, Работники имеют право:

- на полную информацию о своих ПДн и обработке этих данных;
- на свободный бесплатный доступ к своим ПДн, включая право на получение копий любой записи, содержащей ПДн Работника, за исключением случаев, предусмотренных законодательством РФ;
- требовать об исключении или исправлении неверных или неполных ПДн, а также ПДн, обработанных с нарушением требований, определенных законодательством Российской Федерации. При отказе Общества исключить или исправить ПДн Работника, он имеет право заявить в письменной форме Обществу о своем несогласии с соответствующим обоснованием такого несогласия. Работник имеет право дополнить его ПДн оценочного характера заявлением, выражющим его собственную точку зрения;
- требовать об извещении Обществом всех лиц, которым ранее были сообщены неверные или неполные ПДн Работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжаловать в суд любые неправомерные действия или бездействие Общества при обработке и защите его ПДн;
- определять своих представителей для защиты своих ПДн.

7.16. После увольнения Работника его ПДн хранятся Обществом в течение срока, предусмотренного согласием Работника и (или) трудовым договором Работника. В случае если согласием Работника и (или) трудовым договором Работника не определен срок хранения ПДн уволенного Работника, хранение его ПДн осуществляется в течение срока, установленного законодательством.

8. ПРАВИЛА УНИЧТОЖЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Общество обеспечивает уничтожение ПДн в случаях и в сроки, а также в соответствии с требованиями, установленными Законом о персональных данных.

8.2. С целью исключения ошибочного уничтожения содержащих ПДн документов, электронных носителей, а также ПДн в информационных системах, при принятии решения об уничтожении должны учитываться обязательные требования законодательства Российской Федерации в области ПДн и иного законодательства, определяющего случаи и особенности обработки ПДн (налогового

законодательства, законодательства о бухгалтерском учете, законодательства об архивном деле и др.).

8.3. Приготовленные к уничтожению ПДн (их носители) передаются на переработку специализированной организации или уничтожаются в Обществе. Приготовленные к уничтожению ПДн в информационных системах Общества уничтожаются в Обществе.

8.4. Подтверждение факта уничтожения ПДн может фиксироваться путем внесения записи в *Журнале уничтожения персональных данных* или любым иным образом по усмотрению Общества. Форма *Журнала уничтожения персональных данных* содержится в Приложении 2 к настоящему Положению, при этом использование данного журнала не является обязательным.

8.5. В зависимости от типа носителя информации (бумажный или электронный) выделяют два способа уничтожения ПДн:

- физическое уничтожение носителя;
- уничтожение информации с носителя.

8.6. Физическое уничтожение носителя

- Бумажный носитель: используются 2 вида уничтожения – уничтожение через шредирование (измельчение и гидрообработка) и уничтожение через термическую обработку (сжигание).
- Электронный носитель: уничтожение заключается в таком воздействии на рабочие слои дисков, в результате, которого разрушается физическая, магнитная или химическая структура рабочего слоя: механическое разрушение дисков (прессование, механическое эрозирование поверхности - пескоструй, ультразвуковое и электрохимическое эрозирование), химическое травление в агрессивных средах и обжиг или переплавка дисков. Съем данных с магнитных дисков, подвергшихся таким воздействиям, становится невозможным.

8.7. Уничтожение информации с носителя

- Алгоритм уничтожения ПДн основывается на многократной перезаписи в секторах магнитного диска. С физической точки зрения, они основываются на многократном перемагничивании материала записывающей поверхности диска.
- Алгоритмы национальных стандартов предусматривают запись в каждый байт каждого сектора жесткого диска единиц, случайных чисел, а также чисел, дополнительных к записанным на предыдущем проходе. Предполагается несколько перезаписей для одного материального носителя.

8.8. Стандарты уничтожения данных:

- ГОСТ Р50739-95;
- DoD 5220.22-M; NAVSO P-5239-26 (RLL);
- NAVSO P-5239-26 (MFM);
- VSITR.

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

8.10. При необходимости уничтожения или блокирования части ПДн уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению или блокированию.



9. ЛИЦО ОТВЕТСТВЕННОЕ ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. Лицо, ответственное за организацию обработки персональных данных в Обществе, назначается приказом Генерального директора Общества.

9.2. Лицо, ответственное за организацию обработки персональных данных, получает указания непосредственно от Генерального директора Общества и подотчетно ему.

9.3. Лицо, ответственное за организацию обработки персональных данных обязано, помимо прочего:

- осуществлять внутренний контроль за соблюдением Обществом и его Работниками законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн;
- доводить до сведения Работников положения законодательства Российской Федерации о ПДн, локальных актов по вопросам обработки ПДн, требований к защите ПДн и (или) проводить обучение Работников по указанным вопросам;
- организовывать прием и обработку обращений и запросов субъектов ПДн или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

10. ОБЯЗАТЕЛЬСТВА РАБОТНИКОВ О НЕРАЗГЛАШЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1. Работники обязаны:

- не сообщать ПДн Субъекта ПДн третьим лицам без согласия Субъекта ПДн (либо письменного согласия, если Субъектом ПДн является работник), за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью Субъекта ПДн, а также в других случаях, предусмотренных федеральными законами;
- не сообщать ПДн Субъекта ПДн в коммерческих целях без его согласия (либо письменного согласия, если Субъектом ПДн является работник);
- предупредить лиц, получающих ПДн Субъекта ПДн, о том, что эти ПДн могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие ПДн Субъекта ПДн, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен ПДн работников в порядке, установленном федеральными законами;
- осуществлять передачу ПДн Субъекта ПДн в соответствии с локальными нормативными актами Общества;
- разрешать доступ к ПДн Субъекта ПДн только специально уполномоченным лицам (лицам, допущенным к обработке ПДн в соответствии с настоящим Положением), при этом указанные лица должны иметь право получать только те ПДн Субъекта ПДн, которые необходимы для выполнения конкретных функций;
- в отношении работников – не запрашивать информацию о состоянии здоровья, за исключением тех сведений, которые относятся к вопросу о возможности выполнения трудовой функции;

- передавать ПДн работника представителям работников в порядке, установленном федеральными законами, и ограничивать эту информацию только теми ПДн работника, которые необходимы для выполнения указанными представителями их функций;
- в случае не согласованной Обществом попытки третьих лиц получить от Работника информацию о ПДн Субъектов, сообщить незамедлительно о данном факте, с указанием этого третьего лица непосредственному руководителю или Генеральному директору Общества.

11. ПРАВИЛА ДОСТУПА РАБОТНИКОВ В ПОМЕЩЕНИЯ, В КОТОРЫХ ВЕДЕТСЯ ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ, А ТАКЖЕ К МЕСТАМ ХРАНЕНИЯ ДОКУМЕНТОВ, СОДЕРЖАЩИХ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

11.1. При обработке ПДн и хранении документов, содержащих ПДн ("Документы"), должны соблюдаться условия, при которых обеспечивается сохранность ПДн и Документов и исключается несанкционированный доступ к ним.

11.2. При обработке ПДн и хранении Документов также должна исключаться возможность неконтролируемого проникновения и пребывания в помещениях, в которых ведется обработка ПДн ("Помещения"), посторонних лиц и (или) неконтролируемого проникновения в соответствующие места хранения Документов.

11.3. При определении мест хранения Документов необходимо обеспечивать раздельное хранение Документов, содержащих ПДн, обработка которых осуществляется в различных целях.

11.4. Правила, содержащиеся в настоящем разделе, применяются к иным категориям материальных носителей постольку, поскольку иные правила не предусмотрены локальными нормативными актами Общества в отношении соответствующей категории материальных носителей.

11.5. Доступ работников Общества в Помещения организуется на основании *Перечня лиц, допущенных к обработке персональных данных*. Доступ других работников Общества и посетителей в соответствующие Помещения должен осуществляться в сопровождении ответственных работников.

11.6. Нахождение лиц, не являющихся лицами, допущенными к обработке ПДн, в Помещениях возможно только на время, ограниченное необходимостью решения вопросов, связанных с исполнением должностных обязанностей и (или) осуществлением полномочий в рамках договоров, заключенных с соответствующими лицами.

11.7. Во время перерывов в работе, а также после окончания работы с Документами необходимо убирать Документы с поверхности рабочих столов в запирающееся хранилище (сейф, шкаф).

11.8. В нерабочее время Помещения и (или) защищаемые места хранения Документов должны быть закрыты блокирующими средствами в целях предотвращения проникновения посторонних лиц.

11.9. Помещения и (или) места хранения Документов также должны быть закрыты в рабочее время в случае ухода ответственного лица и Работников, постоянно работающих в таком Помещении либо постоянно работающих с такими местами хранения Документов.

11.10. Обеспечение режима безопасности в защищаемом Помещении и контроль за правильностью использования установленных в нем технических средств осуществляется всеми работниками, которые постоянно в нем работают.

11.11. Повседневный контроль за выполнением требований по защите Помещений и (или) мест хранения Документов осуществляют лица, назначенные ответственными за обеспечение

безопасности в отношении указанного Помещения или места хранения Документов согласно *Перечню мест хранения документов, содержащих персональные данные.*

11.12. Периодический контроль эффективности мер защиты Помещений и мест хранения Документов осуществляется лицом, ответственным за организацию обработки ПДн в Обществе.

12. ПРАВИЛА РАССМОТРЕНИЯ ЗАПРОСОВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

12.1. Субъекты ПДн могут обращаться в Общество для получения информации, касающейся обработки их ПДн, уточнения их ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а в иных случаях, предусмотренных Законом о персональных данных (далее- "Запрос").

12.2. В течение тридцати дней с даты получения Запроса Субъекта ПДн или его представителя Общество обязано:

- сообщить Субъекту ПДн или его представителю информацию о наличии ПДн относящихся к соответствующему Субъекту ПДн, а также предоставить возможность ознакомления с этими ПДн; либо
- в случае отказа в предоставлении информации о наличии ПДн о соответствующем Субъекте ПДн или ПДн Субъекту ПДн или его представителю дать в письменной форме мотивированный ответ, содержащий ссылку на положение действующего законодательства, являющееся основанием для такого отказа.

12.3. Запрашиваемые сведения должны быть предоставлены Субъекту ПДн в доступной форме, и в них не должны содержаться ПДн, относящиеся к другим Субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн.

12.4. Запрос считается исполненным, если уполномоченными лицами приняты все необходимые меры по предоставлению ответа, а также выданы исчерпывающие ответы на все вопросы, указанные в Запросе.

12.5. Общество вправе отказать Субъекту ПДн в выполнении Запроса, не соответствующего требованиям, предусмотренным действующим законодательством. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении Запроса лежит на Обществе.

12.6. Общество обязано уведомить Субъекта ПДн или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым ПДн этого Субъекта ПДн были переданы.

12.7. Запросы Субъектов ПДн и ответов Общества на Запросы должны регистрироваться в *Журнале учета обращений субъектов персональных данных*, форма которого содержится в Приложении 3 к настоящему Положению.

12.8. Ответственность за ведение делопроизводства по Запросам, а также за сохранность Запросов возлагается на лицо, ответственное за организацию обработки персональных данных в Обществе либо иным лицом, уполномоченным Генеральным директором Общества. Рассмотрение Запросов может осуществляться с привлечением иных лиц, допущенных к обработке соответствующих категорий ПДн.

12.9. Все поступившие Запросы регистрируются в *Журнале учета обращений субъектов персональных данных* в день их поступления.

13. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ

13.1. В целях осуществления внутреннего контроля соответствия обработки ПДн применимым требованиям в Обществе организовывается проведение периодических (плановых) проверок условий обработки ПДн.

13.2. Ответственным за проведение внутренних проверок соблюдения законодательства о ПДн в надлежащие сроки и за надлежащее оформление результатов указанных проверок является лицо, ответственное за организацию обработки персональных данных в Обществе.

13.3. Плановые внутренние проверки соблюдения законодательства о ПДн проводятся не реже, чем один раз в 3 года.

13.4. Для организации и проведения проверки могут привлекаться подрядные организации.

13.5. Плановая проверка должна быть завершена не позднее, чем через месяц со дня принятия решения о ее проведении.

13.6. Локальными нормативными актами об обеспечении безопасности ПДн при их обработке в информационных системах персональных данных могут быть предусмотрены иные сроки или периодичность проведения отдельных мероприятий по проверке соблюдения законодательства о ПДн.

13.7. По решению Генерального директора Общества или лица, ответственного за организацию обработки персональных данных, а также на основании поступившего письменного заявления о нарушениях правил обработки ПДн (в т.ч. от субъекта ПДн, контролирующих органов) могут проводиться внеплановые проверки соблюдения законодательства о ПДн. Сроки проведения внеплановых проверок и перечень мероприятий в рамках таких проверок определяются в соответствующем приказе Генерального директора Общества.

13.8. Ответственный за организацию обработки персональных данных имеет право в ходе проверки запрашивать у Работников информацию, необходимую для реализации полномочий.

13.9. По результатам проведенной проверки составляется *Акт внутренней проверки* с описанием выявленного соответствия/несоответствия требованиям к обработке ПДн, а также предписания по устранению нарушений. Форма *Акта по итогам проведения внутренней проверки* содержится в Приложении 4 к настоящему Положению. Кроме того, по результатам проверки лицо, ответственное за обработку персональных данных вправе:

- принимать меры по приостановлению или прекращению обработки ПДн, осуществляющейся с нарушением требований законодательства Российской Федерации;
- требовать от уполномоченных на обработку персональных данных должностных лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем ПДн;
- вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности ПДн при их обработке;
- вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки ПДн.



14. ПРАВИЛА ОЦЕНКИ ВОЗМОЖНОГО ВРЕДА СУБЪЕКТАМ ПДн В СЛУЧАЕ НАРУШЕНИЯ ТРЕБОВАНИЙ ПО ОБРАБОТКЕ И ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

14.1. Вред Субъекту ПДн возникает в результате неправомерного или случайного доступа к ПДн, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

14.2. Перечисленные неправомерные действия определяются как следующие нарушения безопасности ПДн:

- Неправомерное предоставление, распространение и копирование ПДн являются нарушением конфиденциальности ПДн.
- Неправомерное уничтожение и блокирование ПДн является нарушением доступности ПДн.
- Неправомерное изменение ПДн является нарушением целостности ПДн.
- Нарушение права субъекта требовать от оператора уточнения его ПДн, их блокирования или уничтожения является нарушением целостности ПДн.
- Нарушение права субъекта на получение информации, касающейся обработки его ПДн, является нарушением доступности ПДн.
- Обработка ПДн, выходящая за рамки установленных и законных целей обработки, в объёме больше необходимого для достижения установленных и законных целей и дольше установленных сроков является нарушением конфиденциальности ПДн.
- Неправомерное получение ПДн от лица, не являющегося субъектом ПДн, является нарушением конфиденциальности ПДн.
- Принятие решения, порождающего юридические последствия в отношении субъекта ПДн или иным образом затрагивающие его права и законные интересы, на основании исключительно автоматизированной обработки его ПДн без согласия на то в письменной форме субъекта ПДн или непредусмотренное федеральными законами, является нарушением конфиденциальности ПДн.
- Публикация ПДн в открытом доступе является нарушением конфиденциальности ПДн.
- Использование ПДн в криминальных целях является нарушением конфиденциальности ПДн.

14.3. Субъекту ПДн может быть причинён вред в форме убытков и морального вреда.

14.4. При оценке возможного вреда Общество исходит из следующего способа учёта последствий допущенного нарушения принципов обработки ПДн:

- Низкий уровень возможного вреда – последствия нарушения принципов обработки ПДн включают только нарушение целостности ПДн, либо только нарушение доступности ПДн;
- Средний уровень возможного вреда – последствия нарушения принципов обработки ПДн включают только нарушение целостности ПДн, повлекшее убытки и моральный вред, либо только нарушение доступности ПДн, повлекшее убытки и моральный вред, либо только нарушение конфиденциальности ПДн;
- Высокий уровень возможного вреда – во всех остальных случаях.

– Низкий уровень возможного вреда – последствия нарушения принципов обработки ПДн включают только нарушение целостности ПДн, либо только нарушение доступности ПДн;

14.5. Оценка возможного вреда субъектам ПДн осуществляется лицом, ответственным за организацию обработки ПДн в Обществе, в соответствии с методикой, описанной выше.

14.6. Состав реализуемых Обществом мер, направленных на обеспечение выполнения обязанностей, предусмотренных Законом о персональных данных, определяется лицом, ответственным за организацию обработки ПДн в Обществе, исходя из правомерности и разумной достаточности указанных мер.

14.7. Оценка возможного вреда субъектам ПДн, связанного с использованием информационных систем ПДн, может осуществляться в соответствии с локальными нормативными актами об обеспечении безопасности ПДн при их обработке в информационных системах ПДн и применимым законодательством.

14.8. Результаты оценки возможного вреда субъектам ПДн в случае нарушения требований по обработке и обеспечению безопасности ПДн в Обществе фиксируются в *Акте оценки возможного вреда субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных*.

15. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ ИНФОРМАЦИИ, СВЯЗАННОЙ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

15.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн, несут дисциплинарную, материальную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством.

16. ФОРМЫ ЖУРНАЛОВ, СВЯЗАННЫХ С ОРГАНИЗАЦИЕЙ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

16.1. Ответственность за ведение и сохранность *Журнала учета ознакомления с правилами обработки персональных данных*, *Журнала уничтожения персональных данных* и *Журнала учета обращений субъектов персональных данных* (далее совместно – "Журналы") возлагается на лицо, ответственное за организацию обработки ПДн в Обществе (либо иное лицо, назначенное Генеральным директором Общества). Ведение Журналов может осуществляться с привлечением иных сотрудников, допущенных к обработке соответствующих категорий ПДн

16.2. Хранение каждого из Журналов осуществляется в течение 5 (пяти) лет с 1 января года, следующего за годом окончания его делопроизводства.

16.3. При ведении Журналов должны соблюдаться следующие условия:

- копирование содержащейся в Журналах информации не допускается;
- ПДн каждого субъекта ПДн могут заноситься в соответствующий Журнал не более одного раза в каждом случае.

16.4. Обработка ПДн, связанная с соблюдением требований настоящего Положения, осуществляется без использования средств автоматизации следующими способами: сбор, запись, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление, доступ), удаление, уничтожение ПДн, за исключением копирования.