УТВЕРЖДАЮ

Генеральный директор
АО «Дирекция Юго-Западного

района»

А.П. Славкин

М.П.

Дата

ПОЛИТИКА

безопасности персональных данных
АО «Дирекция Юго-Западного района»

На 13 листах

Действует с Дата

Оглавление

ВВЕДЕНИЕ

«Политика безопасности персональных данных в АО «Дирекция Юго-Западного района» (далее – Политика) определяет стратегию защиты персональных данных, обрабатываемых в ИСПДн АО «Дирекция Юго-Западного района» и формулирует основные принципы и механизмы защиты ПДн.

Политика является основным руководящим документом АО «Дирекция Юго-Западного района», определяющим требования, предъявляемые к обеспечению безопасности ПДн.

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Настоящий документ разработан в соответствии с требованиями Федерального закона от 27 июля 2006г. № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 11 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Цель и область применения политики

Целью Политики является обеспечение безопасности персональных данных, а также реализация положений нормативных правовых актов и иных документов по защите персональных данных.

Основными целями обеспечения безопасности персональных данных являются:

- предотвращение нарушений прав субъекта персональных данных (физического лица) на сохранение конфиденциальности информации, обрабатываемой в ИСПДн АО «Дирекция Юго-Западного района»;
- предотвращение искажения или несанкционированной модификации информации, содержащей персональные данные, обрабатываемой в ИСПДн АО «Дирекция Юго-Западного района»;

- предотвращение несанкционированных действий по блокированию информации, содержащей персональные данные.

Требования настоящей Политики обязательны для всех сотрудников АО «Дирекция Юго-Западного района» и распространяются на:

- автоматизированные системы АО «Дирекция Юго-Западного района»;
- средства телекоммуникаций;
- информационные ресурсы и носители информации;
- помещения.

Внутренние документы АО «Дирекция Юго-Западного района», затрагивающие вопросы, рассматриваемые в данном документе, должны разрабатываться с учетом положений Политики и не противоречить им.

Настоящий документ является локальным нормативным актом Общества и вступает в силу с момента подписания Генеральным директором АО «Дирекция Юго-Западного района» приказа о введении его в действие.

1.2. Правовое основание обработки персональных данных

Правовым основанием обработки персональных данных являются следующие законодательные акты:

- Федеральный закон от 27.07.2006 года № 152-ФЗ «О персональных данных».

1.3. Законодательство Российской Федерации в области персональных данных

Основными законодательными и нормативно-правовыми актами Российской Федерации в области персональных данных являются:

- Федеральный закон от 12.12.2005 г. №160 "О ратификации конвенции совета Европы о защите физических лиц при автоматизированной обработке персональных данных".
- Федеральный закон от 27.07.2006 года № 152-ФЗ «О персональных данных».
- Постановление Правительства Российской Федерации от 17.11.2007 г. №781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».
- Постановление Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

- Постановление Правительства Российской Федерации от 06.07.08 №512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г.
- Приказ ФСБ от 10 июля 2014 года N 378 Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности.
- Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. Утверждены руководством 8 Центра ФСБ России 21 февраля 2008 г. №149/5-144.
- Приказ ФСТЭК от 18 февраля 2013 года N 21 Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных.
- Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при обработке в информационных системах персональных данных. Утверждены руководством 8 Центра ФСБ России 21 февраля 2008 г. №149/6/6-622.
- Приказ ФСТЭК от 11 февраля 2013 года N 17 Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах.

1.4. Принципы обработки персональных данных

Обработка персональных данных осуществляется на основе принципов:

- законности целей и способов обработки персональных данных и добросовестности;
- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Общества;

- соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

1.5. Способы обработки персональных данных

Общества может осуществлять обработку персональных данных с использованием средств автоматизации, а также без использования таких средств.

2. СУБЪЕКТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Обществом (оператором персональных данных) осуществляется обработка персональных данных следующих категорий субъектов персональных данных:

- Физические лица.

2.1. Цели обработки персональных данных

Обработка персональных данных Общества осуществляется с целью отбора граждан для участия в региональном проекте «Новая жизнь».

2.2. Сроки хранения персональных данных

Период хранения и обработки персональных данных определяется в соответствии со ст.21 Закона «О персональных данных». Обработка ПДн начинается с момента поступления персональных данных в ИСПДн и прекращается:

- в случае выявления неправомерных действий с персональными данными в срок, не превышающий трех рабочих дней с даты такого выявления, Общество устраняет допущенные нарушения. В случае невозможности устранения допущенных нарушений Общества в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, уничтожает персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных Общество уведомляет субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, Общество уведомляет также указанный орган;

- в случае достижения цели обработки персональных данных Общество незамедлительно прекращает обработку персональных данных и уничтожает соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки персональных данных, и уведомляет об этом субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, Общество уведомляет также указанный орган;
- в случае отзыва субъектом персональных данных согласия на обработку своих персональных данных Общество прекращает обработку персональных данных и уничтожает персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва. Об уничтожении персональных данных Общество уведомляет субъекта персональных данных.
- в случае прекращения деятельности Общества.

3. КАТЕГОРИИ ПЕРСОНАЛЬНЫХ ДАННЫХ

В информационных системах Общества осуществляется обработка следующих категорий персональных данных:

- категория 2 – персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1.

3.1. Специальные категории персональных данных.

В информационных системах Общества запрещена обработка следующих персональных данных:

- специальных категорий персональных данных касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, судимости;
- персональных данных о частной жизни, о членстве субъектов персональных данных в общественных объединениях или их профсоюзной деятельности.

Обработка специальных категорий персональных данных может осуществляться в следующих случаях:

- субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;
- персональные данные являются общедоступными;

- персональные данные относятся к состоянию здоровья субъекта персональных данных и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц, и получение согласия субъекта персональных данных невозможно;
- обработка персональных данных необходима в связи с осуществлением правосудия;
- обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством Российской Федерации.

Обработка специальных категорий персональных данных, осуществлявшаяся в вышеперечисленных случаях, должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка.

4. УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

При обработке персональных данных должны соблюдаться следующие условия:

4.1. Конфиденциальность персональных данных

В Обществе документально оформляется перечень сведений конфиденциального характера.

В соответствии с Указом Президента Российской Федерации от 06.03.1997 г. №188 «Об утверждении перечня сведений конфиденциального характера», персональные данные относятся к конфиденциальной информации.

Обществом и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных, за исключением следующих случаев:

- в случае обезличивания персональных данных;
- в отношении общедоступных персональных данных.

4.2. Поручение обработки персональных данных третьему лицу

В случае, если Общество на основании договора поручает обработку персональных данных другому лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке.

Контроль выполнения настоящего требования осуществляет Генеральный директор Общества.

4.3. Хранение и уничтожение персональных данных

Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

Для уничтожения персональных данных, приказом Генерального директора назначается комиссия по уничтожению персональных данных.

Уничтожение персональных данных оформляется актом.

4.4. Обработка персональных данных в целях продвижения товаров, работ, услуг

Обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, допускается только при условии предварительного согласия субъекта персональных данных.

4.5. Трансграничная передача персональных данных

Обществом может осуществляться трансграничная передача персональных данных.

Для осуществления трансграничной передачи персональных данных необходимо получить согласие субъекта персональных данных в письменной форме.

Трансграничная передача персональных данных может осуществляться без согласия субъекта персональных данных в случаях:

- исполнения договора, стороной которого является субъект персональных данных;
- защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.

5. ОБЩИЕ ТРЕБОВАНИЯ ПО ОРГАНИЗАЦИИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Общие положения

Организация работ по обеспечению безопасности персональных данных осуществляется Генеральным директором.

Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах Общества, приказом Генерального директора назначено, ответственное лицо за обеспечение безопасности персональных данных.

Приказом Генерального директора Общества назначаются ответственные лица по работе с персональными данными.

Лица, доступ которых к персональным данным, обрабатываемым в информационных системах, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании утвержденного списка.

5.2. Мероприятия по обеспечению безопасности персональных данных при автоматизированной обработке

5.2.1. Система защиты персональных данных

Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии.

При обработке персональных данных в информационных системах Общества должно быть обеспечено:

- проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
- 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 за обеспечением уровня защищенности персональных данных.

5.2.2. Перечень мероприятий по обеспечению безопасности персональных данных

Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

- определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

- разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;
- проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;
- установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;
- обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
- учет лиц, допущенных к работе с персональными данными в информационной системе;
- контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;
- описание системы защиты персональных данных.

5.3. Контроль и надзор за выполнением требований настоящей Политики

Контроль и надзор за выполнением требований настоящей Политики осуществляется в соответствии с «Планом внутренних проверок состояния защиты персональных данных».

Контроль заключается в проверке выполнения требований нормативных документов по защите информации, а также в оценке обоснованности и эффективности принятых мер. Он может проводиться структурным подразделением, ответственным за обеспечение безопасности персональных данных, или на договорной основе сторонними организациями, имеющими лицензии на деятельность по технической защите конфиденциальной информации.

6. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ТРЕБОВАНИЙ НАСТОЯЩЕЙ ПОЛИТИКИ

Лица, виновные в нарушении требований настоящего Положения, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

ЛИСТ ОЗНАКОМЛЕНИЯ

№	Фамилия и инициалы	Дата	Подпись
1.			
2.			
3.			
4.			
5.			
6.			
7.			