

Утверждено
Приказом № 20 от 30 декабря 2015 года



Генеральный директор
ООО МФО «НАДЕЖНЫЙ ИНВЕСТОР»

К. А. Трегубенко

**ПОЛИТИКА
ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ
ООО МФО «НАДЕЖНЫЙ ИНВЕСТОР»**

(вводится в действие с 01 января 2016 года)

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Цели и сфера действия Политики

1.1.1. В настоящей Политике определены цели обработки персональных данных, установлены общие требования к обеспечению безопасности персональных данных, обрабатываемых ООО МФО «НАДЕЖНЫЙ ИНВЕСТОР» (далее – Компания) с использованием средств автоматизации или без использования таких средств, основные задачи, функции и права подразделения, в обязанности которого входит проведение работ по организации защиты персональных данных. Под обработкой персональных данных понимаются действия (операции) с персональными данными, включающие: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных.

1.1.2. Политика разработана в соответствии с законодательством Российской Федерации в области персональных данных.

1.1.3. Действие Политики распространяется на все структурные подразделения Компании. 1.1.4. Политика является локальным нормативным актом Компании и вступает в силу с момента подписания ее Генеральным директором Компании.

1.2 Принципы обработки персональных данных.

1.2.1. Обработка персональных данных должна осуществляться на основе принципов:

- законности и справедливой основы;
- ограничения обработки персональных данных достижением конкретных, заранее определенных и законных целей;
- недопущения обработки персональных данных, несовместимой с целями сбора персональных данных;
- недопущения объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- обработки только тех персональных данных, которые отвечают целям их обработки;
- соответствия содержания и объема обрабатываемых персональных данных заявленным целям обработки;
- недопущения обработки персональных данных, избыточных по отношению к заявленным целям их обработки;
- обеспечения точности, достаточности и актуальности персональных данных по отношению к целям обработки персональных данных;
- уничтожения либо обезличивания персональных данных по достижении целей их обработки или в случае утраты необходимости в достижении этих целей, при невозможности устранения Компанией допущенных нарушений персональных данных, если иное не предусмотрено федеральным законом.

1.3 Способы обработки персональных данных

1.3.1. Компания осуществляет обработку персональных данных с использованием средств автоматизации, а также без использования таких средств.

1.3.2. Перечень действий с персональными данными, которые осуществляются Компанией при обработке персональных данных субъектов:

- сбор;
- запись;
- систематизация;
- накопление;
- хранение;
- уточнение (обновление, изменение);
- извлечение;
- использование;
- передача (в том числе распространение, предоставление, доступ);
- обезличивание;
- блокирование;
- уничтожение.

1.4 Условия обработки персональных данных

Компания производит обработку персональных данных при наличии хотя бы одного из следующих условий:

- обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;
- обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

- обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;
- обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;
- обработка персональных данных 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 персональных данных;
- осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее – общедоступные персональные данные);
- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

2. СУБЪЕКТЫ И КАТЕГОРИИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ЦЕЛИ ОБРАБОТКИ

2.1 Категории субъектов персональных данных Компанией осуществляется обработка персональных данных следующих категорий субъектов персональных данных:

- кандидаты, претендующие на замещение вакантных должностей;
- работники, состоящие и состоявшие в трудовых отношениях с Компанией;
- члены семей (близких родственников) работников;
- клиенты, состоящие и состоявшие в договорных отношениях с Компанией;

2.2 Категории персональных данных субъектов персональных данных

2.2.1. В информационных системах Компании осуществляется обработка персональных данных не относящихся к:

- специальным категориям персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, судимости;
- сведениям, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность (биометрические персональные данные);
- персональным данным о частной жизни, о членстве субъектов персональных данных в общественных объединениях или их профсоюзной деятельности.

2.2.2. Обработка Компанией специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, допускается в случаях, если:

- субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;
- персональные данные сделаны общедоступными субъектом персональных данных;
- обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, законодательством Российской Федерации о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;
- обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;
- обработка персональных данных необходима для установления или осуществления прав субъекта персональных данных или третьих лиц, а равно в связи с осуществлением правосудия;
- обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством.

2.2.3. Обработка специальных категорий персональных данных должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась их обработка, если иное не установлено федеральным законом.

2.2.4. Обработка персональных данных о судимости может осуществляться Компанией исключительно в случаях и в порядке, которые определяются в соответствии с федеральными законами.

2.2.5. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность – биометрические персональные данные – могут обрабатываться Компанией только при наличии согласия в письменной форме субъекта.

2.3 Цели обработки персональных данных

2.3.1. Обработка персональных данных работников Компании может осуществляться с целью обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

2.3.2. Обработка персональных данных клиентов Компании осуществляется с целью заключения договоров микрозайма и соглашений, исполнения таких договоров и соглашений, принятия решений или совершения иных действий, порождающих юридические последствия (включая решения о предоставлении или отказе в предоставлении микрозайма), предоставления информации об оказываемых Компанией услугах и оказания таких услуг.

2.3.3. Обработка персональных данных клиентов может осуществляться третьими лицами, которые по договору с Компанией осуществляют деятельность по обеспечению погашения долгниками в пользу Компании просроченной задолженности.

3. УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Обработка персональных данных осуществляется с согласия субъектов персональных данных. Та часть персональных данных, которая относится к субъектам, которые начали договорные отношения с Компанией до вступления в силу Федерального закона № 152-ФЗ «О персональных данных», обрабатывается Компанией без получения дополнительного согласия от субъекта, в силу подпунктов 5 и 7 пункта 1 статьи 6 Федерального закона №152-ФЗ «О персональных данных».

3.2. При обработке персональных данных обеспечивается их конфиденциальность, т.е. созданы условия, не допускающие их распространения без согласия субъекта персональных данных, за исключением случаев, когда персональные данные относятся к обезличенным или общедоступным.

3.3. В целях информационного обеспечения в Компании могут создаваться общедоступные источники персональных данных субъектов, в том числе справочники и адресные книги. В общедоступные источники персональных данных с письменного согласия субъекта могут включаться его фамилия, имя, отчество, дата и место рождения, должность, номера контактных телефонов, адрес электронной почты и иные персональные данные, сообщаемые субъектом персональных данных. Сведения о субъекте должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта либо по решению суда или иных уполномоченных государственных органов.

3.4. Компания вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора. В случае если Компания 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, а также других требований Федерального закона №152-ФЗ «О персональных данных».

3.5. Передача персональных данных субъектов третьим лицам может осуществляться только при наличии письменного согласия субъекта, если иное не предусмотрено федеральным законодательством.

3.6. Передача персональных данных субъектов между подразделениями Компании должна осуществляться только между работниками, допущенными к обработке персональных данных.

3.7. Хранение персональных данных осуществляется не дольше, чем этого требуют цели их обработки. Персональные данные подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении, если иное не предусмотрено Законодательством Российской Федерации.

3.8. Хранение персональных данных субъектов осуществляется на бумажных и машинных носителях информации в специально выделенных хранилищах подразделений Компании, а также в информационных системах Компании, обеспечивающих сохранность персональных данных и их защиту от несанкционированного доступа.

3.9. Компания не осуществляет обработку персональных данных в целях политической агитации.

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

3.11. Компания обязана убедиться в том, что иностранным государством, на территорию которого предполагается осуществлять передачу персональных данных, обеспечивается адекватная защита прав субъектов персональных данных, до начала осуществления такой передачи. Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав

субъектов персональных данных, может осуществляться в случаях: – наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных; – исполнения договора, стороной которого является субъект персональных данных.

3.12. Уничтожение персональных данных в информационных системах, на машинных и бумажных носителях информации должно производиться в течение тридцати дней с даты достижения цели обработки (предельного срока хранения) персональных данных.

3.13. Уничтожение персональных данных производится специально назначенной комиссией с обязательным составлением акта.

3.14. Персональные данные при их обработке без использования средств автоматизации обособляются от иной информации путем фиксации их на отдельных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков). 3.15. При фиксации персональных данных на материальных носителях не допускается запись на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. При обработке различных категорий персональных данных без использования средств автоматизации для каждой категории персональных данных должен использоваться отдельный материальный носитель.

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

3.17. 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.

3.18. 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.

3.19. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть 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.

Под блокированием персональных данных понимается временное прекращение операций по их обработке по требованию Клиента при выявлении им недостоверности обрабатываемых сведений или неправомерных по мнению субъекта персональных данных действий в отношении его данных. Компания обязана блокировать персональные данные или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Компании), в случае: - предоставления субъектом персональных данных сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту персональных данных и обработку которых осуществляет Компания, являются неполными, неточными, неактуальными, незаконно полученными или не являются необходимыми для заявленной цели обработки; - выявления неправомерной обработки персональных данных Компанией при обращении или по запросу субъекта персональных данных или его представителя, либо уполномоченного органа по защите прав субъектов персональных данных. Блокирование персональных данных в информационных системах Компании в случаях осуществляется на основании письменного заявления субъекта персональных данных. Блокирование персональных данных в информационных системах персональных данных производится ответственными по информационной безопасности (администраторами безопасности) этих систем на основании сообщения руководителя подразделения Компании, имеющих право обработки персональные данные, направляемого с использование корпоративной электронной почты.

4. ПРАВА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Субъект персональных данных имеет право на получение у Компании информации, касающейся обработки его персональных данных, если такое право не ограничено в соответствии с федеральными законами.

4.2. Субъект персональных данных вправе требовать от Компании уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав. Компания обязана немедленно прекратить по требованию субъекта персональных данных обработку его персональных данных в вышеуказанных целях.

4.3. Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных федеральными законами, или при наличии согласия в письменной форме субъекта персональных данных.

4.4. Если субъект персональных данных считает, что Компания осуществляет обработку его персональных данных с нарушением требований «О персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Компании в Уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

4.5. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

5. ОСОБЕННОСТИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1 Общие положения

5.1 Компания обрабатывает и хранит персональные данные на электронных носителях, на бумажных носителях в виде персонализированных рукописных бланков и возвратных форм (далее – Формы).

5.2 Обработка Форм

5.2.1.Обработка Форм может включать в себя следующие действия: – нанесение персональных данных на Формы машинным (тиографским) способом; – сканирование Форм; – ручная и полуавтоматическая сортировка Форм без сканирования; – неавтоматизированное чтение Форм; – ввод персональных данных с Форм в электронный вид силами операторов; – хранение Форм.

5.2.2.Все указанные выше операции могут включать обработку персональных данных на бумажных носителях.

5.2.3.Все указанные выше операции совершаются уполномоченными сотрудниками Компании либо на основе Договоров уполномоченными третьими лицами - подрядчиками Компании. Непременным условием работы, регламентируемой такими договорами, является исполнение сторонами требований «О персональных данных».

5.2.4.В случае если указанные выше операции выполняются с персональными данными в бумажном виде, производственный процесс организован таким образом, что каждый сотрудник Компании (или подрядчика Компании), имеющий доступ к персональным данным, не может иметь доступ к персональным данным более чем 10000 субъектов персональных данных.

5.2.5.Мерами, обеспечивающими адекватную защиту указанных персональных данных, являются: – учет сотрудников, обрабатывающих персональные данные; – регистрация доступа сотрудников к персональным данным (ведение журнала); – учет действий сотрудников, задействованных в переводе персональных данных из бумажной формы в электронную; – упаковка бумажных носителей, количество которых превышает соответствующее 10000 субъектам, в непрозрачные упаковочные материалы так, чтобы обеспечить физическую невозможность несанкционированного доступа к указанным персональным данным; – видеонаблюдение и видеозапись в помещениях, где производится обработка и хранение персональных данных на бумажных носителях в объемах, превышающих 10000 субъектов.

5.3 Получение персональных данных клиентов Компании

5.3.1.Продукция и услуги Компании распространяются обычным способом посредством личного участия Клиента, обращающегося за выдачей микрозайма к Компании. 5.3.2.Согласие участника осуществляется путем подписания им заявления-анкеты либо отдельного документа, содержащего согласие на обработку персональных данных.

5.3.3.В соответствии с пунктом 1 статьи 9 согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме.

5.3.4. Дав свое согласие обработку персональных данных, участник подтверждает, что является дееспособным совершеннолетним гражданином РФ, сообщившим собственные и достоверные персональные данные.

5.3.5. Согласие участника дает Компании право осуществлять сбор, хранение, обработку и использование персональных данных участника для исполнения договора микрозайма.. 5.3.6. В случае поступления в адрес Компании заявления от клиента с требованием о блокировке (уничтожении) его персональных данных, представитель Компании принимает все необходимые процедурные действия для выполнения требования обратившегося лица, кроме тех случаев, когда обработка персональных данных необходима для исполнения договора с клиентом, стороной которого, либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта

персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем (на основании ст. 6, п. 1, ч. 5 Федерального закона № 152-ФЗ).

5.5 Обработка персональных данных кандидатов на вакантные должности

Персональные данные кандидатов обрабатываются исключительно с целью их подбора на замещение вакантных должностей Компании. Перечень персональных данных кандидатов: – фамилия, имя, отчество; – дата и место рождения; – паспортные данные; – пол; – сведения о семейном положении; – сведения об образовании; – сведения о стаже работы; – сведения о предыдущих местах работы; – сведения о воинском учете; – сведения о водительском удостоверении; – номер контактного телефона; – адрес электронной почты. Срок хранения документов лиц, не принятых на работу, (анкеты, автобиографии, заявления, рекомендательные письма, резюме и др.) в соответствии со ст. 663 приказа Министерства культуры РФ от 25.08.2010 № 558 «Об утверждении «Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения» (далее – приказ Минкультуры № 558) составляет три года. От кандидата должно быть получено письменное согласие на обработку его персональных данных Компанией. В случаях, когда Компания может получить необходимые персональные данные кандидата только у третьей стороны, Компания должна уведомить об этом кандидата и получить от него письменное согласие.

5.6 Обработка персональных данных работников

Персональные данные работников обрабатываются с целью их трудоустройства, обучения, продвижения по службе, охраны труда и личной безопасности работников, контроля качества выполняемой работы, оплаты труда в соответствие с требованиями законов и иных нормативных документов, а также обеспечения сохранности имущества Компании. Перечень персональных данных работников: – фамилия, имя, отчество; – дата и место рождения; – паспортные данные; – адреса мест регистрации и фактического проживания; – сведения о семейном положении и составе семьи; – сведения об образовании и о повышении квалификации; – сведения о трудовом и общем стаже работы; – сведения о предыдущих местах работы; – сведения о воинском учете; – сведения о водительском удостоверении; – номер страхового свидетельства; – ИНН; – номер контактного телефона; – адрес электронной почты; – сведения о заработной плате работника; – сведения о социальных льготах; – занимаемая должность; – фотография. В соответствии с приказом Минкультуры № 558 личное дело, лицевой счет и личная карточка уволенного работника на бумажных носителях информации хранятся до достижения предельного срока архивного хранения – 75 лет со дня увольнения работника. Остальные документы кадрового учета на бумажных носителях, содержащие персональные данные работников, хранятся в соответствии с приказом Минкультуры № 558 в течение пяти лет со дня увольнения работника. Хранение персональных данных уволенного работника в информационной системе персональных данных и на машинных носителях информации в соответствии со ст. 196 Гражданского кодекса Российской Федерации осуществляется до истечения срока взаимной исковой давности – трех лет со дня увольнения работника. На основании ч. 1 ст. 6 ФЗ-152 обработка персональных данных работника может осуществляться Компанией без его письменного согласия. Получение согласия работника необходимо в следующих случаях: – для получения персональных данных у третьей стороны; – для передачи персональных данных третьей стороне; – для перевода определенных персональных данных в категорию общедоступных; – для обработки специальных категорий персональных данных; – для обработки биометрических персональных данных; – для использования персональных данных в целях продвижения товаров, работ, услуг, а также в целях политической агитации; – при поручении обработки персональных данных другому лицу; – при необходимости принятия на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия; – при необходимости трансграничной передачи персональных данных (если такая передача осуществляется не во исполнение договора, стороной которого является работник).

5.7 Обработка персональных данных членов семьи.

Персональные данные членов семьи обрабатываются с целью выполнения трудового законодательства в отношении работника Компании, а также обеспечения получения страховых выплат при наступлении несчастного случая с работником. Перечень персональных данных членов семьи: – фамилия, имя, отчество; – степень родства; – год рождения; – номер контактного телефона. В соответствии с ТК РФ Компанией в интересах членов семьи могут обрабатываться на бумажных носителях персональные данные членов семьи об инвалидности, беременности и другие специальные категории персональных данных. Поскольку персональные данные членов семьи обрабатываются в составе персональных данных работника, сроки их обработки и хранения соответствуют п. 2.3. настоящего Положения. В соответствии с ч. 1, ст. 6 и ч. 2 ст. 10 ФЗ-152 допускается обработка персональных данных членов семьи без получения их согласия.

6. МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1 Общие положения

- 6.1.1. Мероприятия по обеспечению безопасности персональных данных являются составной частью деятельности Компании.
- 6.1.2. Безопасность персональных данных, обрабатываемых Компанией, обеспечивается реализацией правовых, организационных и технических мер, необходимых для обеспечения требований федерального законодательства в области защиты персональных данных.
- 6.1.3. Организация работ по обеспечению безопасности персональных данных осуществляется руководством Компании.
- 6.1.4. Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах Компании, приказом Генерального директора назначается сотрудник организации, отвечающий за отдельные направления работ в рамках обеспечения безопасности персональных данных.
- 6.1.5. Для выбора и реализации методов и способов защиты информации может привлекаться организация, имеющая оформленную в установленном законодательством РФ порядке лицензию на осуществление деятельности по технической защите конфиденциальной информации.
- 6.1.6. Для предотвращения несанкционированного доступа к персональным данным Компанией применяются следующие организационно-технические меры: – назначение должностных лиц, ответственных за организацию обработки и защиты персональных данных; – ограничение состава лиц, имеющих доступ к персональным данным; – ознакомление субъектов с требованиями федерального законодательства и нормативных документов Компании по обработке и защите персональных данных; – организация учета, хранения и обращения носителей информации; – определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз; – разработка на основе модели угроз системы защиты персональных данных; – проверка готовности и эффективности использования средств защиты информации; – разграничение доступа пользователей к информационным ресурсам и программно-аппаратным средствам обработки информации; – регистрация и учет действий пользователей информационных систем персональных данных; – использование антивирусных средств и средств восстановления системы защиты персональных данных; – применение в необходимых случаях средств межсетевого экранирования, обнаружения вторжений, анализа защищенности и средств криптографической защиты информации.

7. ОТВЕТСТВЕННЫЙ ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ.

7.1 Общие положения

7.1.1 В соответствии с п. 1 ст. 18.1 Федерального закона № 152-ФЗ приказом Генерального директора Компании назначен ответственный за организацию обработки персональных данных.

7.1.2 Основной задачей ответственного за организацию обработки персональных данных является обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных Компании путем предотвращения утечки персональных данных по техническим каналам, несанкционированного доступа к ним, предупреждения преднамеренных программно-технических воздействий с целью их разрушения (уничтожения) или искажения в процессе обработки, передачи и хранения.

7.1.3 Свою деятельность ответственный за организацию обработки персональных данных осуществляет в соответствии с «Планом мероприятий по защите персональных данных».

7.1.4 В своей деятельности ответственный за организацию обработки персональных данных руководствуется законодательными и нормативно-правовыми актами Российской Федерации в области защиты персональных данных, настоящей Политикой и иными нормативными актами Компании.

7.2 Функции ответственного за организацию обработки персональных данных

7.2.1 Организация работ по формированию моделей угроз безопасности персональных данных при их обработке в информационных системах персональных данных Компании, в том числе: – оценка полноты и правильности определения угроз безопасности; – плановый и внеплановый пересмотр.

7.2.2 Организация работ по созданию системы защиты персональных данных (комплекса организационно-технических мер), обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем.

7.2.3 Контроль выполнения мероприятий по защите персональных данных, реализуемых в рамках подсистем защиты с учетом класса информационной системы: – антивирусной защиты; – межсетевого экранирования; – управления доступом; – регистрации и учета; – обеспечения целостности; – обнаружения вторжений; – анализа защищенности; – резервного копирования.

7.2.4 Контроль за соответствием эксплуатации информационных систем персональных данных требованиям организационно-технической и эксплуатационной документации.

7.2.5 Контроль соблюдения работниками Компании установленных требований по обеспечению безопасности персональных данных.

7.2.6 Разработка предложений по совершенствованию системы защиты персональных данных.

- 7.2.7 Подготовка материалов для проведения мероприятий по повышению осведомленности работников Компании по вопросам обеспечения безопасности персональных данных.
- 7.2.8 Организация работ по размещению оборудования информационных системы персональных данных в части выполнения требований по сохранности носителей персональных данных и средств защиты информации, а также исключения возможности проникновения и неконтролируемого пребывания посторонних лиц.
- 7.2.9 Организация и проведение работ по обеспечению безопасности помещений, в которых производится обработка персональных данных, а также находятся на хранении материальные носители персональных данных, в том числе выработка мер, необходимых для обеспечения таких условий.
- 7.2.10 В случае необходимости – ведение журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъектов персональных данных в помещения, которых находится структурные подразделения Компании.
- 7.2.11 Обеспечение соответствия обработки персональных данных работников Компании требованиям законодательства в области персональных данных, в частности, требованиям Трудового Кодекса Российской Федерации.
- 7.2.12 Анализ и оценка соответствия внутренних нормативных документов Компании, в части касающейся обработки персональных данных работников Компании, а в случае выявления несоответствий – внесение необходимых изменений, в том числе в должностные инструкции персонала.
- 7.2.13 Организация и проведение работ по обучению (повышению осведомленности) персонала в области персональных данных.
- 7.2.14 Анализ законодательства Российской Федерации в области персональных данных.
- 7.2.15 Оценка выполнения Компанией обязанностей, установленных законодательством Российской Федерации в области персональных данных, а в случае выявления несоответствий - выработка рекомендаций по их устранению.
- 7.2.16 Организация подготовки и направление в уполномоченный орган по защите прав субъектов персональных данных Уведомления об обработке персональных данных, а в случае изменения сведений, содержащихся в Реестре операторов осуществляющих обработку персональных данных – направление сведений о таких изменениях.
- 7.2.17 В случае выявления неправомерных действий с персональными данными направляет уведомление об устранении нарушений.
- 7.2.18 Анализ и оценка соответствия типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, требованиям законодательства Российской Федерации в области персональных данных, а в случае выявления несоответствий - выработка рекомендаций по их устранению.
- 7.2.19 Анализ и оценка соответствия договорной базы Компании требованиям законодательства Российской Федерации в области персональных данных, а в случае выявления несоответствий – внесение соответствующих изменений (дополнений).
- 7.2.20 Контроль выполнения требований законодательства Российской Федерации, в части касающейся согласия субъектов персональных данных на обработку их персональных данных.
- 7.2.21 Организацию работ по созданию специальной комиссии и сбор необходимых документов при прохождении федерального государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных.
- 7.2.22 Эксплуатация информационных систем персональных данных в соответствии с организационно-технической и эксплуатационной документацией.
- 7.2.23 Обеспечение работоспособности системы защиты персональных данных, реализуемой в рамках подсистем защиты с учетом класса информационной системы: – антивирусной защиты; – межсетевого экранирования; – управления доступом; – регистрации и учета; – обеспечения целостности; – обнаружения вторжений; – анализа защищенности; – резервного копирования.
- 7.2.24 Организация мероприятий по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.
- 7.2.25 Организация учета и использования магнитных, оптических и других машинных носителей информации, предназначенных для обработки персональных данных.
- 7.2.26 Организация работ по привлечению сторонних организаций для формирования и сопровождения баз данных и информационного взаимодействия (центров обработки информации), выполняющих функции операторов и администраторов системы централизованной обработки данных.
- 7.2.27 Учет, установка и ввод в эксплуатацию (проведение работ, связанных с монтажом, настройкой и проверкой работоспособности) средств защиты информации в соответствии с эксплуатационной и технической документацией.

7.2.28 Учет лиц, допущенных к работе с персональными данными в информационных системах персональных данных (предоставление на основе заявок прав доступа пользователей к информационным системам персональных данных, учет таких пользователей и предоставленных им прав).

7.2.29 Проверка готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации (средство защиты информации считается готовым к использованию, если оно отвечает требованиям, установленным организационно-технической документацией на информационную систему персональных данных).

7.2.30 Реализация предложений по совершенствованию системы защиты персональных данных.

7.2.31 Организация обучения лиц примен器яющих средства защиты информации, правилам работы с ними.

7.2.32 Обеспечение безопасности персональных данных при их обработке, осуществляющейся без использования средств автоматизации.

7.2.33 Организация работ по уничтожению материальных носителей персональных данных в случае достижения целей обработки или в случае утраты необходимости в их достижении с составлением актов об уничтожении.

7.2.34 Организация работ по ознакомлению работников Компании, осуществляющих обработку персональных данных без использования средств автоматизации, а также лиц, осуществляющих такую обработку по договору с Компанией, о факте обработки ими персональных данных, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки.

7.2.35 Обеспечение раздельного хранения персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

7.2.36 Обеспечение контроля за сохранностью материальных носителей персональных данных.

7.2.37 Анализ исходных данных по информационным системам персональных данных (оценка полноты и правильности).

7.2.38 Присвоение информационным системам соответствующих классов и их документальное оформление.

7.2.39 Контроль выполнения требований настоящей Политики.

7.2.40 Общий контроль соблюдения подразделениями Компании требований по обеспечению безопасности персональных данных и соблюдения требований законодательства в области защиты персональных данных, в том числе: – контроль за порядком предоставления информации (персональных данных) органам власти, физическим и юридическим лицам; – контроль за соблюдением порядка взаимодействия с федеральными органами исполнительной власти по вопросам безопасности персональных данных; – проведение разбирательств и составление заключений по фактам несоблюдения установленных требований.

7.3 Права ответственного за организацию обработки персональных данных. Ответственный за организацию обработки персональных данных, осуществляющие функции по организации защиты персональных данных имеет право на: – запрос и получение необходимых материалов для организации и проведения работ по вопросам обеспечения безопасности персональных данных в Компании. – привлечение к проведению работ по защите персональных данных других подразделений Компании. – привлечение к проведению работ по защите персональных данных на договорной основе сторонних организаций. – контроль деятельности структурных подразделений Компании в части выполнения ими требований по обеспечению безопасности персональных данных. – внесение предложений Генеральному директору Компании о приостановке работ в случае обнаружения несанкционированного доступа, утечки, персональных данных, а также в случае предпосылок нарушения безопасности персональных данных.

8. КОНТРОЛЬ ЗА ВЫПОЛНЕНИЕМ ТРЕБОВАНИЙ ПОЛИТИКИ

8.1. За выполнением требований настоящей Политики осуществляется контроль.

8.2. Перечень мероприятий по контролю, его периодичность, а также ответственные лица за выполнение мероприятий по контролю установлены «Планом проведения контроля обеспечения безопасности персональных данных».

8.3. Контроль заключается в проверке выполнения требований нормативных документов по защите информации, а также в оценке обоснованности и эффективности принятых мер.

8.4. По результатам контроля составляются заключения.

8.5. Мероприятия по контролю могут осуществляться на договорной основе сторонними организациями, имеющими лицензии на право проведения соответствующих работ.

9. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ТРЕБОВАНИЙ НАСТОЯЩЕЙ ПОЛИТИКИ

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