



АДМИНИСТРАЦИЯ ГОРОДА ТОБОЛЬСКА ДЕПАРТАМЕНТ ФИНАНСОВ

ПРИКАЗ

06 сентября 2021г.

№ 79

Об утверждении Политики обработки персональных данных в Департаменте финансов Администрации города Tobольска

В соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами,

П Р И К А З Ы В А Ю:

1. Утвердить Политику обработки персональных данных в Департаменте финансов Администрации города Tobольска согласно приложению к настоящему приказу.

2. Назначить ответственным за организацию обработки персональных данных в Департаменте финансов Администрации города Tobольска начальника отдела информационных технологий и защиты информации Москвина Дмитрия Юрьевича.

3. Разместить утвержденную Политику обработки персональных данных в Департаменте финансов Администрации города Tobольска на официальном сайте Администрации города Tobольска.

4. Приказ Департамента финансов Администрации города Tobольска «Об утверждении Политики обработки персональных данных в Департаменте финансов Администрации города Tobольска» от 10.04.2020г. № 62 считать утратившим силу.

5. Приказ вступает в силу со дня его подписания.

6. Контроль за исполнением настоящего приказа оставляю за собой.

Директор Департамента

Т.А. Шевченко

Политика обработки персональных данных в департаменте финансов Администрации города Тобольска

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Политика определяет порядок обработки персональных данных и меры по обеспечению безопасности персональных данных департамента финансов Администрации города Тобольска (далее - ДФ) с целью защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.2. Политика обработки персональных данных в ДФ разработана в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее - ФЗ от 27.07.2006 № 152-ФЗ) и приказом Федеральной службы по техническому и экспортному контролю России (далее - ФСТЭК России) от 18.02.2013 г. № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.3. Действие Политики распространяется на все персональные данные субъектов, обрабатываемые в ДФ с применением средств автоматизации и без применения таких средств.

1.4. К настоящей Политике должен иметь доступ любой субъект персональных данных.

II. ПРИНЦИПЫ И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАнных

2.1. Обработка персональных данных в ДФ осуществляется на основе следующих принципов:

- законности;
- ограничения обработки персональных данных достижением конкретных, заранее определённых 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 объёма обрабатываемых персональных данных заявленным целям обработки; недопущения обработки избыточных персональных данных 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 ДФ допущенных нарушений персональных данных, если иное не предусмотрено федеральным законом.

2.2. ДФ обрабатывает персональные данные только 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 законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;
- 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 ДФ 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;
- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

2.3. ДФ и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

2.4. В целях информационного обеспечения в ДФ могут создаваться общедоступные источники персональных данных работников, в том числе справочники и адресные книги. В общедоступные источники персональных данных с согласия работника могут включаться его фамилия, имя, отчество, дата и место рождения, должность, номера контактных телефонов, адрес электронной почты.

Сведения о работнике должны быть в любое время исключены из общедоступных источников персональных данных по требованию работника либо по решению суда или иных уполномоченных государственных органов.

2.5. ДФ 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. Лицо, осуществляющее обработку персональных данных по поручению ДФ, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные ФЗ от 27.07.2006 № 152-ФЗ.

2.6. Обработка ДФ 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 установления или осуществления прав субъекта персональных данных или третьих лиц, а равно и в связи с осуществлением правосудия;
- обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о противодействии терроризму, о противодействии коррупции, об исполнительном производстве, уголовно-исполнительным законодательством Российской Федерации;
- обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством.

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

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

2.8. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность - биометрические персональные данные - могут обрабатываться ДФ только при наличии согласия в письменной форме работника.

2.9. Трансграничная передача персональных данных на территории

иностранных государств может осуществляться ДФ только при наличии согласия субъекта персональных данных на трансграничную передачу его персональных данных.

III. ПРАВА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Субъект персональных данных принимает решение о предоставлении его персональных данных и даёт согласие на их обработку свободно, своей волей и в своём интересе. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом.

Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований, указанных в ФЗ от 27.07.2006 № 152-ФЗ, возлагается на ДФ.

3.2. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, если такое право не ограничено в соответствии с федеральными законами. Субъект персональных данных вправе требовать от ДФ 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.

3.3. Обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путём осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации допускается только при условии предварительного согласия субъекта персональных данных. Указанная обработка персональных данных признается осуществляемой без предварительного согласия субъекта персональных данных, если ДФ не докажет, что такое согласие было получено.

ДФ обязан немедленно прекратить по требованию субъекта персональных данных обработку его персональных данных в вышеуказанных целях.

3.4. 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.

3.5. Если субъект персональных данных считает, что ДФ осуществляет обработку его персональных данных с нарушением требований ФЗ № 152 или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие ДФ в

Уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

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.

IV. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Безопасность персональных данных, обрабатываемых ДФ, обеспечивается реализацией правовых, организационных, технических и программных мер, необходимых и достаточных для обеспечения требований федерального законодательства в области защиты персональных данных.

4.2. Для целенаправленного создания в ДФ неблагоприятных условий и труднопреодолимых препятствий для нарушителей, пытающихся осуществить несанкционированный доступ к персональным данным в целях овладения ими, их видоизменения, уничтожения, заражения вредоносной компьютерной программой, подмены и совершения иных несанкционированных действий в ДФ применяются следующие организационно-технические меры:

- назначение должностных лиц, ответственных за организацию обработки и защиты персональных данных;
- ограничение и регламентация состава работников, имеющих доступ к персональным данным;
- ознакомление работников с требованиями федерального законодательства и нормативных документов Администрации по обработке и защите персональных данных;
- обеспечение учёта и хранения материальных носителей информации и их обращения, исключая хищение, подмену, несанкционированное копирование и уничтожение;
- определение угроз безопасности персональных данных при их обработке, формирование на их основе моделей угроз;
- разработка на основе модели угроз системы защиты персональных данных для соответствующего класса информационных систем;
- реализация разрешительной системы доступа пользователей к информационным ресурсам, программно-аппаратным средствам обработки и защиты информации;
- регистрация и учёт действий пользователей информационных систем персональных данных;
- парольная защита доступа пользователей к информационной системе персональных данных;
- применение средств контроля доступа к коммуникационным портам, устройствам ввода-вывода информации, съёмным машинным носителям и внешним накопителям информации;
- применение в необходимых случаях средств криптографической

- защиты информации для обеспечения безопасности персональных данных при передаче по открытым каналам связи и хранении на машинных носителях информации;
- осуществление антивирусного контроля, предотвращение внедрения в корпоративную сеть вредоносных программ (программ-вирусов) и программных закладок;
 - применение межсетевое экранирования;
 - обнаружение вторжений в корпоративную сеть Администрации, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных;
 - централизованное управление системой защиты персональных данных;
 - резервное копирование информации;
 - обеспечение восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
 - обучение работников, использующих средства защиты информации, применяемые в информационных системах персональных данных, правилам работы с ними;
 - учёт применяемых средств защиты информации, эксплуатационной и технической документации к ним;
 - использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
 - проведение мониторинга действий пользователей, проведение разбирательств по фактам нарушения требований безопасности персональных данных;
 - размещение технических средств обработки персональных данных, в пределах охраняемой территории;
 - организация пропускного режима на территорию Администрации города Тобольска;
 - поддержание технических средств охраны, сигнализации помещений в состоянии постоянной готовности.

4.3. При обработке персональных данных в информационных системах персональных данных, проводится оценка эффективности принятых в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных, а также выполняется контроль за реализованными мерами по обеспечению безопасности персональных данных.

4.3.1. До ввода в эксплуатацию информационной системы персональных данных лицо, ответственное за организацию обработки персональных данных в ДФ, организует мероприятия по оценке эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных в информационной системе персональных данных и дает заключение по форме согласно Приложению №1 к настоящей Политике. Указанная оценка проводится не

реже одного раза в 3 года.

V. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

5.1. Иные права и обязанности ДФ, как оператора персональных данных, определяются законодательством Российской Федерации в области персональных данных.

Информация, относящаяся к персональным данным, ставшая известной в связи с реализацией трудовых отношений и в связи с оказанием государственных и муниципальных услуг и осуществлением государственных и муниципальных функций, является конфиденциальной информацией и охраняется законом.

Должностные лица ДФ, виновные в нарушении норм, регулирующих обработку и защиту персональных данных, несут материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, установленном федеральными законами.

Приложение № 1

УТВЕРЖДАЮ
Руководитель (должность)

_____/_____/_____
« ____ » _____ 20__ г.

**ЗАКЛЮЧЕНИЕ ОБ ОЦЕНКЕ ЭФФЕКТИВНОСТИ
реализованных в рамках системы защиты персональных данных
мер по обеспечению безопасности персональных данных
в информационной системе персональных данных**

« _____ »
(наименование информационной системы персональных данных)

Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных (далее – Оценка) в информационной системе персональных данных

« _____ »
(наименование информационной системы персональных данных)

(далее – ИСПДн) соответствует требованиям приказа ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

В ИСПДн разрешается обработка персональных данных.

Оценка действительна в течении 3 (трех) лет с момента утверждения.

Ответственный за организацию
обработки персональных данных

_____/_____/_____
« ____ » _____ 20__ г.