

Государственное бюджетное учреждение
Ярославской области
«ЯРОБЛТРАНСКОМ»
(ГБУ ЯО «Яроблтранском»)

ПРИКАЗ

г. Ярославль

«27» июня 2018 г.

№ 41-А

Об утверждении политики ГБУ ЯО «Яроблтранском» в отношении
обработки персональных данных

На основании Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и в целях определения правил обработки и обеспечения безопасности персональных данных, а также предупреждения угроз информационной безопасности в отношении ГБУ ЯО «Яроблтранском»

П р и к а з ы в а ю:

1. Утвердить Политику ГБУ ЯО «Яроблтранском» в отношении обработки персональных данных (далее - Политика).
2. Работникам ГБУ ЯО «Яроблтранском» при выполнении трудовых обязанностей руководствоваться требованиями, установленными Политикой.
3. Контроль за исполнением приказа возложить на заместителя директора ГБУ ЯО «Яроблтранском» А.В. Алексева.
4. Настоящий приказ вступает в силу со дня его издания.

Директор



А.С. Тимакин



Приложение

УТВЕРЖДЕНА

приказом ГБУ ЯО «Яроблтранском»
от _____ 2018 года № 41-А

ПОЛИТИКА

ГБУ ЯО «Яроблтранском» в отношении обработки персональных данных

1. Общие положения

1.1. Назначение и область действия

Настоящая Политика ГБУ ЯО «Яроблтранском» в отношении обработки персональных данных (далее – Политика) разработана с целью обеспечения защиты прав и свобод субъекта персональных данных при обработке его персональных данных.

Положения Политики определяют правила обработки персональных данных в ГБУ ЯО «Яроблтранском» (далее – Учреждение).

Требования Политики и документов, разработанных на ее основе, распространяются на всех работников Учреждения (штатных, временных, работающих по контракту и т.п.) и прочих лиц (подрядчики, аудиторы и т.п.).

Требования Политики распространяются на все технологические процессы Учреждения, связанные с обработкой персональных данных.

1.2. Основные понятия

В настоящей Политике используются следующие сокращения и термины:

Сокращение	Значение
АС	Автоматизированная система
ИБ	Информационная безопасность
ИС	Информационная система
ИСПДн	Информационная система персональных данных
ОРД	Организационно-распорядительный документ
ПДн	Персональные данные
ПО	Программное обеспечение
ЯО	Ярославская область

Термин	Определение
Блокирование персональных данных	Временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).
Информационная система	Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.
Конфиденциальность персональных данных	Обязанность оператора или иного лица, получившего доступ к персональным данным, не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.
Обезличивание персональных данных	Действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.
Обработка персональных данных	Действия, совершаемые с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.
Оператор персональных данных	Государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.
Персональные данные	Информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных).
Политика	Общие цели и указания, формально выраженные руководством.
Предоставление персональных данных	Действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.
Субъект персональных данных	Физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных.
Уничтожение персональных данных	Действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

1.3. Основания для разработки

Политика разработана во исполнение положений Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Закона) с учетом требований иных нормативных актов Российской Федерации в сфере ИБ.

2. Права и обязанности Оператора персональных данных и Субъекта персональных данных.

2.1. Права и обязанности Оператора персональных данных

Оператор персональных данных (далее – Оператор) вправе:

- получать от Субъекта персональных данных (далее - Субъект) полную, точную и достоверную информацию о составе его ПДн;
- отказать Субъекту в оказании услуг или установлению деловых и/или трудовых взаимоотношений, в случае отказа Субъекта предоставить свои ПДн в соответствии с требованиями нормативных и правовых актов Российской Федерации.

Оператор обязан:

- обрабатывать ПДн в полном соответствии заявленным целям обработки и требованиям законодательства Российской Федерации;
- обеспечивать безопасность ПДн при их обработке;
- предоставлять, а также блокировать и уничтожать имеющиеся сведения о Субъекте в случае его законных требований.

2.2. Права и обязанности Субъекта персональных данных

Субъект вправе:

- требовать от Оператора уточнения его ПДн, 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;
- требовать перечень своих ПДн, обрабатываемых Учреждением и источник их получения;
- получать информацию о сроках обработки своих ПДн, в том числе о сроках их хранения;
- требовать извещения всех лиц, которым ранее были сообщены неверные или неполные его персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.

Субъект обязан:

- передавать для обработки комплекс достоверных, документированных ПДн, состав которых установлен законодательством;
- своевременно сообщать об изменении своих персональных данных.

3. Цели и правовые основания обработки персональных данных

3.1. Цели сбора персональных данных

Целями обработки (сбора) ПДн являются:

- ведение кадровой работы;
- ведение бухгалтерского учета;
- исполнения гражданско-правовых договоров;
- обеспечение транспортной безопасности.

3.2. Правовые основания обработки персональных данных

Правовыми основаниями обработки ПДн являются:

- Трудовой кодекс Российской Федерации;
- Налоговый кодекс Российской Федерации;
- Гражданский кодекс Российской Федерации;
- Федеральный закон от 21.11.1996 № 129-ФЗ «О бухгалтерском учете»;
- Федеральный закон от 15.12.2001 № 167-ФЗ «Об обязательном пенсионном страховании»;
- Федеральный закон от 24.07.2009 № 212-ФЗ «О страховых взносах в Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования и территориальные фонды обязательного медицинского страхования»;
- Приказ Министерства транспорта Российской Федерации от 19.07.2012 № 243 «Об утверждении Порядка формирования и ведения автоматизированных централизованных баз персональных данных о пассажирах, а также предоставления содержащихся в них данных»;
- согласие на обработку ПДн в рамках полномочий Оператора.

4. Категории Субъектов и содержание персональных данных

4.1. Категории субъектов персональных данных

К субъектам персональных данных относятся:

категория 1: работники Оператора, в том числе бывшие работники, кандидаты на замещение вакантных должностей, а также родственники работников;

категория 2: контрагенты Оператора (физические лица);

категория 3: клиенты (пассажиры) Оператора (физические лица);

4.2. Содержание обрабатываемых персональных данных

Для Субъектов, относящихся к категории 1, обрабатываются следующие ПДн:

- реквизиты документа, удостоверяющего личность, ИНН, СНИЛС, номер контактного телефона, состав семьи;
- данные трудовой книжки, страховой номер ПФР, табельный номер;
- данные документов о профессиональной подготовке (переподготовке), повышении квалификации, стажировке, аттестации, подтверждении специальных знаний, присвоении ученой степени, ученого звания;
- дата и причины увольнения;
- информация о кадровых перемещениях;
- данные о воинском учете (категория, звание, состав, годность, военкомат);
- категория застрахованного сотрудника;
- сведения о предоставленных социальных льготах;
- сведения о заработной плате и иных выплатах и удержаниях, получаемых и производимых в процессе трудовой деятельности у оператора, номера банковских карт;
- данные водительского удостоверения (для работников – водителей);
- сведения о временной нетрудоспособности, а также номер и серия листка нетрудоспособности.

Для Субъектов, относящихся к категории 2, обрабатываются следующие ПДн:

- реквизиты документа, удостоверяющего личность, ИНН, СНИЛС, номер контактного телефона;
- данные документов о профессиональной подготовке (переподготовке), повышении квалификации, стажировке, аттестации, подтверждении специальных знаний, присвоении ученой степени, ученого звания;

Для Субъектов, относящихся к категории 3, обрабатываются следующие ПДн:

- фамилия, имя и отчество, дата и место рождения;
- вид и номер документа, удостоверяющего личность.

5. Порядок и условия обработки персональных данных

5.1. Правила обработки персональных данных

Организация обработки и обеспечения безопасности ПДн осуществляется в соответствии с Законом и принятыми в соответствии с ним нормативными правовыми актами.

Разработка мероприятий по обеспечению безопасности ПДн Субъектов находится в компетенции ответственного за организацию обработки ПДн.

Реализацию мероприятий по обеспечению безопасности ПДн Субъектов осуществляет Администратор информационной безопасности.

При необходимости к работам по защите ПДн могут привлекаться другие структурные подразделения Учреждения.

Требования Политики при необходимости уточняются иными локально-правовыми актами Учреждения.

Основными принципами обработки ПДн в Учреждении являются:

- законность целей и способов обработки ПДн;
- соответствие целей обработки ПДн целям, заранее определенным и заявленным при сборе ПДн;
- соответствие объема и характера обрабатываемых ПДн, способов обработки ПДн целям обработки ПДн;
- достоверность ПДн, их достаточность для целей обработки, недопустимость обработки ПДн, избыточных по отношению к целям, заявленным при сборе ПДн;
- недопустимость объединения баз данных ИСПДн, созданных для несовместимых между собой целей;
- хранение ПДн в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки;
- уничтожение ПДн по достижении целей обработки или в случае утраты необходимости в их достижении.

В Учреждении обрабатываются ПДн как с использованием средств автоматизации, так и без использования таковых.

В случае достижения цели обработки ПДн, если иное не предусмотрено законодательством Российской Федерации, Учреждение прекращает обработку ПДн и производит их уничтожение, или обеспечивает прекращение обработки и уничтожение ПДн, которые обрабатывались третьими лицами на основании договора с Учреждением, в порядке, установленном законодательством Российской Федерации. Уничтожение персональных данных и материальных носителей ПДн в Учреждении осуществляется в установленном порядке и документируется.

5.2. Требования к обработке персональных данных

Обработка ПДн в Учреждении должна осуществляться в полном соответствии с требованиями статьи 9 Закона.

Предоставление ПДн Учреждением третьему лицу, кроме случаев, предусмотренных законодательством Российской Федерации, должно осуществляться с согласия субъекта ПДн. В случае если Учреждение на основании договора поручает обработку ПДн третьему лицу, существенным условием договора (или заключенного с таким лицом соглашения о неразглашении конфиденциальной информации) должна являться обязанность указанного лица по обеспечению конфиденциальности ПДн и безопасности ПДн при их обработке, а также выполнение им требований, предъявляемых к защите ПДн в соответствии со статьей 19 Закона и несение ответственности перед Учреждением за обработку таких ПДн.

В Учреждении ведется учет работников, осуществляющих обработку ПДн. Работник, ответственный за ведение учета, назначается приказом директора Учреждения. Учет ведется на основе установленных ролей в соответствии с занимаемой должностью и/или списков доступа к ИСПДн.

Работники Учреждения, осуществляющие обработку ПДн, должны быть проинформированы о факте обработки ими ПДн и категориях, обрабатываемых ПДн, а также должны быть ознакомлены с требованиями по обеспечению безопасности ПДн, содержащимися во внутренних нормативных документах.

При обработке ПДн на бумажных носителях следует руководствоваться Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным постановлением Правительства Российской Федерации от 15.09.2008 № 687.

5.3. Мероприятия по обеспечению безопасности персональных данных

Объектами защиты являются сами ПДн, информационные технологические процессы и АС, обрабатывающие ПДн.

Безопасность ПДн достигается путем реализации комплекса мероприятий, позволяющих минимизировать риск нарушения информационной безопасности Учреждения.

Безопасность ПДн при их обработке в ИСПДн Учреждения обеспечивается посредством системы защиты ПДн.

Система защиты ПДн включает организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности ПДн.

Выбор требований по обеспечению безопасности ПДн осуществляется в соответствии с требованиями законодательства Российской Федерации в области данных в зависимости от установленного уровня защищённости ПДн, зафиксированного в соответствующем акте классификации.

Ответственный за обработку ПДн обеспечивает ведение перечня обрабатываемых ПДн на основе утвержденных актов классификации.

В Учреждении вводятся ограничения на доступ в помещения, в которых проводится обработка ПДн, и устанавливаются требования к учету, хранению и уничтожению материальных носителей ПДн.

Обеспечение конфиденциальности ПДн не требуется в случае обезличивания ПДн и в отношении общедоступных ПДн.

5.4. Мероприятия по обеспечению прав субъектов персональных данных

Учреждение рассматривает все обращения Субъектов в обязательном порядке.

Порядок обработки обращений и запросов Субъектов (или их законных представителей) по вопросам обработки их ПДн и действий в случае запросов уполномоченного органа по защите прав Субъектов или иных надзорных органов, осуществляющих контроль и надзор в области ПДн, устанавливается во внутренних нормативных документах Учреждения.

В случае отзыва Субъектом ПДн согласия на обработку его ПДн, если иное не предусмотрено законодательством Российской Федерации, Учреждение обязано прекратить их обработку или обеспечить прекращение такой обработки.

Хранение ПДн осуществляется в форме, позволяющей определить Субъекта, не дольше чем этого требуют цели обработки ПДн, если иной срок хранения не установлен федеральным законом.

В случае, если хранение ПДн далее не требуется для целей обработки ПДн, Учреждение должно уничтожить ПДн или обеспечить их уничтожение в порядке, установленном нормативными актами Учреждения и законодательством Российской Федерации.

5.5. Обязанности работников, обрабатывающих персональные данные

Работники, допущенные к обработке ПДн, обязаны:

- знать и неукоснительно выполнять требования настоящей Политики;
- обрабатывать ПДн только в рамках выполнения своих должностных обязанностей;
- не разглашать ПДн, полученные в результате выполнения своих должностных обязанностей, а также ставшие им известными по роду своей деятельности;
- пресекать действия других лиц, которые могут привести к разглашению или искажению ПДн, а также уничтожению ПДн вне установленного порядка;
- выявлять факты разглашения или искажения ПДн, а также уничтожения ПДн вне установленного порядка, и информировать ответственного за организацию обработки ПДн.

Обязанности работников, допущенных к обработке ПДн, регламентируются внутренними нормативными документами Учреждения, устанавливающими правила обращения с конфиденциальной информацией.

6. Ответственность

Ответственность за выполнение правил по обработке ПДн возлагается на всех работников Учреждения.

Ответственность работников Учреждения за несоблюдение требований Политики, повлекшее за собой разглашение, утрату или нарушение целостности ПДн, определяется законодательством Российской Федерации, внутренними нормативными документами, а также трудовыми договорами и должностными инструкциями работников Учреждения.

7. Контроль и пересмотр

Осуществление общего контроля за соблюдением правил, установленных настоящей Политикой, предоставление рекомендаций по их выполнению, а также поддержание настоящей Политики и связанных с ней документов в актуальном состоянии, возлагается на ответственного за организацию обработки ПДн. Все изменения, внесённые в настоящую Политику, должны учитываться в листе «История изменений» (Приложение № 1).

