

Утверждено Приказом Генерального  
Директора ООО «Компания «Домоком»  
№2/попд от 01.07.2015 г.  
«Об утверждении Положения об обработке  
документов в области Персональных данных»

**Положение об обработке персональных данных  
в ООО «Компания «Домоком»**

Редакция №1 от 01.06.2015г.

## **1 Общие положения**

### **1.1 Цели и сфера действия Положения**

Положение об обработке персональных данных (далее – Положение) определяет требования к порядку обработки и защите (обеспечению безопасности) персональных данных субъектов, персональные данные которых обрабатываются ООО «Компания «Домоком» (далее – Компания) с использованием средств автоматизации или без использования таких средств.

Целью настоящего Положения является соблюдение прав и свобод человека и гражданина при обработке его персональных данных в информационных системах Компании, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Мероприятия по обеспечению безопасности персональных данных являются составной частью деятельности Компании.

Действие Положения распространяется на все структурные подразделения Компании.

Настоящий документ является локальным нормативным актом Компании и вступает в силу с момента утверждения его Приказом Генерального директора.

### **1.2. Законодательство Российской Федерации в области персональных данных**

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

- Конституция Российской Федерации.
- Федеральный закон от 19.12.2005 №160-ФЗ «О ратификации конвенции совета Европы о защите физических лиц при автоматизированной обработке персональных данных».
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
- Постановление Правительства Российской Федерации от 17.11.2007 №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 №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».
- Приказ Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации, Министерства информационных технологий и связи Российской Федерации от 13.02.2008 №55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных».
- Приказ Федеральной службы по техническому и экспортному контролю от 05.02.2010 № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах 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.
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена Заместителем директора ФСТЭК России 14 февраля 2008 г.
- 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.

### **1.3. Принципы обработки персональных данных**

Обработка персональных данных осуществляется на основе принципов:

- 1) законности целей и способов обработки персональных данных и добросовестности;
- 2) соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Компании, как оператора персональных данных;
- 3) соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- 4) достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- 5) недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

### **1.4. Способы обработки персональных данных**

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

### **1.5. Условия обработки персональных данных**

При обработке персональных данных должны соблюдаться следующие условия.

### **1.6. Конфиденциальность персональных данных**

В Компании документально оформляется перечень сведений конфиденциального характера.

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

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

- 1) в случае обезличивания персональных данных;
- 2) в отношении общедоступных персональных данных.

### **1.7. Поручение обработки персональных данных третьему лицу**

В случае если Компания на основании договора поручает обработку персональных данных другому лицу, существенным условием договора является наличие права у данного лица на обработку персональных данных, обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке.

Контроль выполнения настоящего требования осуществляет лицом ответственным за организацию обработки персональных данных.

### **1.8. 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.

Места хранения материальных носителей персональных данных утверждаются Приказом Генерального директора.

### **1.9. 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.

### **1.10. Трансграничная передача персональных данных**

Компанией не осуществляется трансграничная передача персональных данных.

### **1.11. Взаимодействие с федеральными органами исполнительной власти**

Взаимодействие с федеральными органами исполнительной власти по вопросам обработки и защиты персональных данных субъектов, персональные данные которых обрабатываются Компанией, осуществляется в рамках законодательства Российской Федерации.

## **2. Субъекты и категории персональных данных**

### **2.1. Субъекты персональных данных**

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

- 1) абоненты – физические лица, которых связывают с Компанией договорные отношения об оказании услуг связи, а также конечные пользователи абонентов-юридических лиц;
- 2) работники – физические лица, вступившие в трудовые отношения с работодателем<sup>1</sup>;
- 3) пользователи систем контроля и управления доступом<sup>2</sup> – физические лица, в отношении которых осуществляются мероприятия по контролю доступа на защищаемые объекты Компании<sup>3</sup>.

### **2.2. Категории персональных данных**

В информационных системах Компании осуществляется обработка следующих категорий персональных данных:

**Категория 2:** персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию;

**Категория 3:** персональные данные, позволяющие идентифицировать субъекта персональных данных;

**Категория 4:** обезличенные и (или) общедоступные персональные данные.

### **2.3. Специальные категории персональных данных.**

В информационных системах Компании запрещена обработка следующих персональных данных:

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

---

<sup>1</sup> Ст. 20, ТК РФ

<sup>2</sup> Далее – Посетители

<sup>3</sup> п.3.20. ГОСТ Р 53110-2008

Обработка специальных категорий персональных данных может осуществляться в следующих случаях:

- 1) субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;
- 2) персональные данные являются общедоступными;
- 3) 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;

Компания не запрашивает и не обрабатывает персональные данные, относящиеся к состоянию здоровья субъекта персональных данных, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

- 4) обработка персональных данных необходима в связи с осуществлением правосудия;
- 5) 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.

### **3. Мероприятия по обеспечению безопасности персональных данных**

#### **3.1. Общие положения**

Организация работ по обеспечению безопасности персональных данных осуществляется руководством Компании.

Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах Компании, приказом Генерального директора назначаются лица ответственные за обеспечение безопасности персональных данных.

Лица, ответственные за обеспечение безопасности персональных данных, в своей деятельности руководствуется «Положением об обработке персональных данных» и действующим законодательством.

Разработка и осуществление мероприятий по обеспечению безопасности персональных данных может осуществляться также сторонними организациями на договорной основе, имеющими лицензии на право проведения соответствующих работ.

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.

#### **3.2. Мероприятия по обеспечению безопасности персональных данных при автоматизированной обработке**

##### **3.2.1. 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 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 Компании 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 над обеспечением уровня защищенности персональных данных.

### **3.2.2. 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 над 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.

### **3.2.3. Классификация информационных систем персональных данных**

Информационные системы персональных данных Компании подлежат обязательной классификации.

Для проведения классификации информационных систем персональных данных Компании приказом Генерального директора назначается комиссия.

Результаты классификации оформляются соответствующим актом.

### **3.2.4. Помещения, в которых ведется обработка персональных данных**

Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты

информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

### **3.3. Мероприятия по обеспечению безопасности персональных данных при их обработке без использования средств автоматизации**

Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных, либо имеющих к ним доступ.

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

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе работники Компании или лица, осуществляющие такую обработку по договору с Компанией), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки.

### **3.4. Контроль и надзор за выполнением требований настоящего Положения**

Контроль и надзор за выполнением требований настоящего Положения 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.

### **3.5. Финансирование мероприятий по обеспечению безопасности персональных данных**

Финансирование мероприятий по обеспечению безопасности персональных данных осуществляется за счет средств Компании и предусматривается бюджетом Компании.

## **4. Ответственность за нарушение требований настоящего положения**

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

## **5. Персональные данные абонентов Компании**

### **5.1. Цели обработки персональных данных**

Обработка персональных данных абонентов Компании осуществляется с целью исполнения обязательств по договорам об оказании услуг связи.

### **5.2. Перечень обрабатываемых персональных данных**

Состав персональных данных абонентов Компании определяется содержанием предоставляемых абонентами анкетных данных при заполнении инфокарты, а также документов, необходимых для заключения и обеспечения договоров об оказании услуг связи в соответствии с п.14 Постановления Правительства РФ от 27 августа 2005 г. N 538 «Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность», а также законодательством о связи.

### **5.3. Сроки хранения персональных данных**

Срок хранения персональных данных абонентов Компании определяется ст.196 Гражданского Кодекса Российской Федерации «Общий срок исковой давности» и составляет три года после расторжения договора.

## **6. Персональные данные работников Компании**

Персональные данные работника – информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника<sup>4</sup>

### **6.1. Цели обработки персональных данных**

Обработка персональных данных работников Компании осуществляется 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<sup>5</sup>.

### **6.2. Перечень обрабатываемых персональных данных**

Состав персональных данных работников Компании определяется ст. 65 Трудового Кодекса Российской Федерации: при заключении трудового договора лицо, поступающее на работу, предъявляет работодателю:

- Паспорт или иной документ, удостоверяющий личность.
- Трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства.
- Страховое свидетельство государственного пенсионного страхования.
- Документы воинского учета - для военнообязанных и лиц, подлежащих призыву на военную службу.
- Документ об образовании, о квалификации или наличии специальных знаний - при поступлении на работу, требующую специальных знаний или специальной подготовки.

Запрещается требовать от лица, поступающего на работу, документы помимо предусмотренных Трудовым кодексом, иными федеральными законами, указами Президента Российской Федерации и постановлениями Правительства Российской Федерации.

### **6.3. Сроки хранения персональных данных**

Выписка из перечня типовых управленческих документов, образующихся в деятельности организаций, с указанием сроков хранения, утвержденного Руководителем Федеральной архивной службы России 06.10.2000:

## **8. КАДРОВОЕ ОБЕСПЕЧЕНИЕ**

### **8.1. Прием, перемещение (перевод), увольнение работников**

№ статьи 337 Личные дела (заявления, автобиографии, копии приказов и выписки из них, копии личных документов, характеристики, листки по учету кадров, анкеты, аттестационные листы и др.):

а) руководителя организации; членов руководящих, исполнительных, контрольных органов организации; работников, имеющих государственные и иные звания, премии, награды, ученые степени и звания - Постоянно

б) работников - 75 лет (ЭПК)

№ статьи 338 Трудовые договоры (контракты), трудовые соглашения, не вошедшие в состав личных дел - 75 лет (ЭПК)

№ статьи 339 Личные карточки работников (в том числе временных работников) -75 лет (ЭПК)

<sup>4</sup> Ст 85 ТК РФ

<sup>5</sup> Ст 86 п1 ТК РФ



№ статьи 340 Характеристики работников, не имеющих личных дел - 75 лет (ЭПК)

№ статьи 341 Документы (анкеты, автобиографии, листки по учету кадров, заявления, рекомендательные письма, резюме и др.) лиц, не принятых на работу - 1 год

№ статьи 342 Подлинные личные документы (трудовые книжки, дипломы, аттестаты, удостоверения, свидетельства) - До востребования; Не востребованные - не менее 50 лет.

№ статьи 343 Документы (справки, докладные и объяснительные записки, копии приказов, выписки из приказов, заявления, командировочные удостоверения и др.), не вошедшие в состав личных дел - 5 лет

№ статьи 358 Книги, журналы, карточки учета:

а) приема, перемещения (перевода), увольнения работников - 75 лет

б) работников, направленных в командировки - 5 лет

в) военнообязанных - 3 года; После увольнения

г) отпусков - 3 года

д) личных дел, личных карточек, трудовых договоров (контрактов), трудовых соглашений - 75 лет

е) выдачи трудовых книжек и вкладышей к ним - 50 лет

ж) выдачи справок о заработной плате, стаже, месте работы - 3 года

з) выдачи командировочных удостоверений - 5 лет

## **7. Сроки хранения персональных данных**

В соответствии с целями обработки персональных данных Посетителей, а именно в соответствии с целью обеспечения личной безопасности работников и сохранности имущества Компании, срок хранения персональных данных Посетителей определяется ст.196 Гражданского Кодекса Российской Федерации «Общий срок исковой давности» и составляет три года.

## **Термины и определения**

**Персональные данные** - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

**Оператор** - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

**Обработка персональных данных** - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

**Распространение персональных данных** - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

**Использование персональных данных** - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

**Блокирование персональных данных** - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

**Уничтожение персональных данных** - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

**Обезличивание персональных данных** - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

**Информационная система персональных данных** - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

**Конфиденциальность персональных данных** - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

**Трансграничная передача персональных данных** - передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

**Общедоступные персональные данные** - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.