Утверждено Приказом генерального директора

№_____ от _____

Положение об обработке персональных данных

в ООО «ЭЛЛКО»

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 «ЭЛЛКО» (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».

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. 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.

1.8. 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.

2.1. 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[1];

[1] Ст. 20, ТК РФ

3) пользователи систем контроля доступа[2] - физические лица, в отношении которых осуществляются мероприятия по контролю доступа на охраняемые объекты Компании[3].

4) Посетители официального сайта Компании – физические лица, осуществляющие предоставление персональных данных с использованием информационно-телекоммуникационных сетей, при пользовании опцией «Подключайся».

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).

---

[2] Далее – Посетители
[3] п.3.2. ГОСТ Р 53110-2008

- Персональных данных о частной жизни, о членстве субъектов персональных данных в общественных объединениях или их профсоюзной деятельности.

Обработка специальных категорий персональных данных может осуществляться в следующих случаях:

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.

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 структурные подразделения, ответственные за обеспечение безопасности персональных данных.

Подразделения, ответственные за обеспечение безопасности персональных данных, в своей деятельности руководствуется настоящим Положением.

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. 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.

Порядок и правила доступа в помещения Компании устанавливаются «Положением о пропускном режиме».

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), 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 за выполнением требований настоящего Положения 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. Обработка персональных данных абонентов

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 Правилами оказания услуг телефонной связи (Постановление Правительства РФ от 09 декабря 2014 г. № 1342), Правилами оказания телематических услуг связи (Постановление Правительства РФ от 10 сентября 2007 г. № 575) данными, предоставляемыми абонентами при заполнении, заявлений, анкет (в случае их заполнения), 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. Обработка персональных данных работника - информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника[3]

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

[3] Ст 85 ТК РФ

безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества[4].

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:

[4] Ст 86 п1 ТК РФ

Сроки хранения документов

Таблица

Номер статьи	Вид документа	Срок хранения	Примечание
8. КАДРОВОЕ ОБЕСПЕЧЕНИ		**Е**	
8.1. Прием, перемещение (перевод), увольнение работников			
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)	
338	Трудовые договоры (контракты), трудовые соглашения, не вошедшие в состав личных дел	75 лет (ЭПК)	
339	Личные карточки работников (в том числе временных работников)	75 лет (ЭПК)	
340	Характеристики работников, не имеющих личных дел	75 лет (ЭПК)	

Номер статьи	Вид документа	Срок хранения	Примечание
341	Документы (анкеты, автобиографии, листки по учету кадров, заявления, рекомендательные письма, резюме и др.) лиц, не принятых на работу	1 год	
342	Подлинные личные документы (трудовые книжки, дипломы, аттестаты, удостоверения, свидетельства)	До востребования	Не востребованные - не менее 50 лет.
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	
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. Обработка персональных данных пользователей систем контроля доступа

7.1. Цели обработки персональных данных

Обработка персональных данных Посетителей осуществляется с целью предоставления однократного и (или) неоднократного пропуска субъектов персональных данных на территорию, на которой находятся подразделения Компании, а также с целью обеспечения личной безопасности работников и сохранности имущества Компании. Обработка

персональных данных Посетителей может осуществляться Компанией только с согласия субъекта персональных данных.

7.2. Перечень обрабатываемых персональных данных

В состав персональных данных пользователей систем контроля и управления доступом входят:

1) сведения о личности владельца паспорта[5]:
   - фамилия;
   - имя;
   - отчество;
   - пол;
   - дата рождения;
   - место рождения.
2) фотография владельца паспорта.

7.3. 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.

[5] «Описание бланка паспорта гражданина Российской Федерации»

8. Обработка персональных данных посетителей официального сайта Компании

8.1. Цели обработки персональных данных

Обработка персональных данных Посетителей официального сайта осуществляется с целью обработки заявок на подключение к услугам связи потенциальных абонентов Компании. Обработка персональных данных Посетителей может осуществляться Компанией только с согласия субъекта персональных данных.

8.2. Перечень обрабатываемых персональных данных

В состав персональных данных посетителя сайта, воспользовавшегося опцией «Подключайся» входят

- имя;
- телефонный номер;
- почтовый адрес места нахождения;
- адрес электронной почты;

8.3. Сроки хранения персональных данных

В соответствии с целями обработки персональных данных Посетителей, срок хранения персональных данных Посетителей определяется ст.196 Гражданского Кодекса Российской Федерации «Общий срок исковой давности» и составляет три года.

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.