

**Правила обработки персональных данных
в ООО «ЖилКомИнкасо-Нижний Новгород»**

1. Общие положения

1.1. Настоящие Правила обработки персональных данных в ООО «ЖилКомИнкасо-Нижний Новгород» (далее - Правила) разработаны в соответствии с Конституцией Российской Федерации, Федеральным законом от 27.06.2006 N 152-ФЗ "О персональных данных", Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и защите информации», Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», Постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при обработке в информационных системах персональных данных», Постановлением Правительства Российской Федерации от 06.07.2008 №512 «Об утверждении Требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных», Приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 5 сентября 2013 г. N 996 "Об утверждении требований и методов по обезличиванию персональных данных"; и иными нормативными правовыми актами Российской Федерации, а также Правилами внутреннего трудового распорядка ООО «ЖилКомИнкасо-Нижний Новгород».

1.2. Персональные данные субъекта персональных данных ООО «ЖилКомИнкасо-Нижний Новгород» (далее - Общество) при обработке его персональных данных без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).

1.3. При фиксации персональных данных субъекта персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных субъектов персональных данных, цели обработки которых заведомо не совместимы.

1.4. Лица, осуществляющие обработку персональных данных субъекта персональных данных Общества без использования средств автоматизации либо имеющих к ним доступ, информируются о факте обработки ими персональных данных субъекта персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных действующим законодательством РФ.

2. Основные понятия

2.1. **Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

2.2. **Субъект персональных данных** - физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных.

2.3. **Обработка персональных данных** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу

(распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

2.4. Обработка персональных данных без использования средств автоматизации - обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

2.5. Информационные системы персональных данных (далее - ИСПДн) - совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации.

2.5. 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;

2.6. Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

2.7. Деобезличивание - действия, в результате которых обезличенные данные принимают вид, позволяющий определить их принадлежность конкретному субъекту персональных данных, то есть становятся персональными данными

2.8. Обезличенные данные - это данные, хранимые в информационных системах в электронном виде, принадлежность которых конкретному субъекту персональных данных невозможно определить без дополнительной информации.

2.9. Обработка обезличенных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации, с обезличенными данными, без применения их предварительного деобезличивания.

3. Правила обработки персональных данных без использования средств автоматизации

3.1. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).

3.2. Места хранения материальных носителей персональных данных определяются в соответствии со списком, утверждаемым приказом.

3.3. Обмен и передача персональных данных при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических средств. Сотрудники осуществляют обработку, включая сбор, накопление, систематизацию, уточнение и передачу персональных данных в объемах и целях, предусмотренных законодательством Российской Федерации и локальными нормативными актами Общества, также обеспечивают их защиту от неправомерного использования, утраты и несанкционированного уничтожения.

3.4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, должны соблюдаться следующие условия:

3.4.1. документы должны содержать сведения о цели обработки персональных данных, наименование и адрес Общества, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

3.4.2. документы должны предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, либо должно быть получено отдельное предварительное письменное согласие на обработку персональных данных;

3.4.3. документы должны быть составлены таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

3.4.4. документы должны исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

3.5. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению отдельной обработки персональных данных, в частности:

3.5.1. при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

3.5.2. при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

3.6. Правила, предусмотренные пунктами 3.4. и 3.5. настоящих Правил, применяются также в случае, если необходимо обеспечить отдельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

3.7. 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 (удаление, вымарывание).

3.8. Уточнение персональных данных субъекта персональных данных при осуществлении их обработки 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 субъекта персональных данных.

3.9. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

3.9.1. правил хранения бумажных носителей;

3.9.2. правил доступа к ним и в помещения, где они хранятся.

3.10. При достижении целей обработки персональных данных материальные носители персональных данных должны быть уничтожены или переданы в архив.

4. Правила обработки персональных данных, осуществляемой в информационных системах персональных данных

4.1. Общество обеспечивает конфиденциальность и безопасность персональных данных при их обработке в ИСПДн.

4.2. Безопасность персональных данных при их обработке в ИСПДн обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства,

средства предотвращения несанкционированного доступа к персональным данным, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Для обеспечения безопасности персональных данных при их обработке в ИСПДн осуществляется защита речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.

4.3. Обмен персональных данных при их обработке в ИСПДн осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических средств.

4.4. Размещение ИСПДн, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должна обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц. Порядок доступа работников или иных лиц в помещения, определен Положением о защите персональных данных работников и Положением о защите персональных данных пациентов.

4.5. При обработке персональных данных в ИСПДн Общества обеспечивается:

4.5.1. проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

4.5.2. своевременное обнаружение фактов несанкционированного доступа к персональным данным;

4.5.3. недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

4.5.4. возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

4.5.5. постоянный контроль за обеспечением уровня защищенности персональных данных.

4.6. Системный администратор - организация, привлекаемая по гражданско-правовому договору:

4.6.1. осуществляет периодическое обновление антивирусных пакетов и контролирует их работоспособность;

4.6.2. проводит периодическое тестирование всего установленного программного обеспечения на предмет отсутствия компьютерных вирусов. При обнаружении компьютерного вируса работник Общества, осуществляющий обработку персональных данных, обязан немедленно поставить в известность администратора и прекратить какие-либо действия в ИСПДн;

4.6.3. проводит, в случае необходимости, лечение зараженных файлов, после чего вновь проводит антивирусный контроль;

4.6.4. в случае обнаружения вируса, не поддающегося лечению, прекращается использование ГДМ. При обнаружении на ЖДМ вируса, не поддающегося лечению, администратор обязан поставить в известность руководство, прекратить работу в ИСПДн и в возможно короткие сроки обновить пакет антивирусных программ;

4.7. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение: парольной политики; антивирусной политики; правил работы со съемными носителями (если они используются); правил резервного копирования; правил доступа в помещения, где расположены элементы информационных систем.

5. Правила обезличивания персональных данных

5.1. Обезличивание персональных данных обеспечивает защиту от несанкционированного использования персональных данных субъектов персональных данных, а также возможность их

обработки. Обезличивание персональных данных производится с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, при достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством Российской Федерации.

5.2. Для обезличивания персональных данных применяются способы, не противоречащие действующему законодательству, при условии дальнейшей обработки персональных данных к таким относятся:

- 5.2.1. уменьшение перечня обрабатываемых сведений;
- 5.2.2. замена части сведений идентификаторами;
- 5.2.3. обобщение - понижение точности некоторых сведений;
- 5.2.4. понижение точности некоторых сведений (например, «Место жительства» может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только город)
- 5.2.5. деление сведений на части и обработка в разных информационных системах;
- 5.2.6. другие способы.

5.3. Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации. Обработка обезличенных данных осуществляется с использованием технических и программных средств, соответствующих форме представления и хранения данных. При обезличивании персональных данных не допускается совместное хранение персональных данных и обезличенных данных.

5.4. Обезличивание персональных данных субъектов производится Обществом перед внесением их в информационную систему.

5.5. Общество вправе обрабатывать в информационной системе обезличенные данные, полученные от третьих лиц.

5.6. В процессе обработки обезличенных данных может проводиться деобезличивание. После обработки, персональные данные, полученные в результате такого деобезличивания, уничтожаются.

5.7. Порядок обезличивания персональных данных:

5.7.1. Ответственное лицо принимает решение о необходимости обезличивания персональных данных;

5.7.2. Лица, непосредственно осуществляющие обработку персональных данных, готовят предложения по обезличиванию персональных данных, обоснование такой необходимости и способ обезличивания;

5.8. Обезличенные персональные данные не подлежат разглашению и нарушению правил конфиденциальности информации, установленных Положением о защите персональных данных.

6. Блокировка и уничтожение персональных данных

6.1. Порядок блокировки и разблокировки персональных данных:

6.1.1. Блокировка персональных данных субъекта персональных данных осуществляется с письменного заявления субъекта.

6.1.2. Блокировка персональных данных подразумевает:

6.1.2.1. Запрет распространения персональных данных любыми средствами (e-mail, сотовая связь, материальные носители).

6.1.2.3. Использование персональных данных в рассылках (sms, e-mail, почта) с письменного согласия субъекта персональных данных.

6.1.2.4. Изъятие бумажных документов, относящихся к субъекту персональных данных и содержащих его персональные данные из внутреннего документооборота Общества и запрет их использования.

6.1.3. Блокировка персональных данных субъекта может быть временно снята, если это требуется для соблюдения законодательства РФ.

6.1.4. Разблокировка персональных данных осуществляется с письменного согласия (при наличии необходимости получения согласия) или заявления субъекта персональных данных.

6.1.5. Повторное согласие субъекта на обработку его персональных данных (при необходимости его получения) влечет разблокирование его персональных данных.

6.2. Порядок уничтожения персональных данных:

6.2.1. Уничтожение персональных данных субъекта персональных данных подразумевает прекращение какого-либо доступа к персональным данным субъекта.

6.2.2. При уничтожении персональных данных субъекта работники Общества не могут получить доступ к персональным данным субъекта в информационных системах.

6.2.3. Способы уничтожения персональных данных: бумажные носители разрезаются (уничтожаются с помощью аппарата шредера), персональные данные в информационных системах обезличиваются, с электронного носителя информация стирается с помощью программных или технических средств, которые гарантируют уничтожение информации, также возможно механическое уничтожение электронных носителей информации

6.2.4. Бумажные носители документов при уничтожении персональных данных уничтожаются. Персональные данные восстановлению не подлежат.

6.2.5. Операция уничтожения персональных данных необратима.

6.2.6. Срок, после которого возможна операция уничтожения персональных данных субъекта, определяется окончанием срока обязательного хранения документации, содержащей персональные данные, установленного законодательством Российской Федерации.

6.2.7. Уничтожение носителей персональных данных осуществляется специально сформированной комиссией и оформляется Актом уничтожения персональных данных (Приложение № 1).

6.2.8. Акт составляется отдельно на каждый способ уничтожения носителей.

6.2.9. Все листы акта, а также все произведенные исправления и дополнения в акте заверяются подписями всех членов комиссии.

7. Меры по обеспечению безопасности персональных данных

7.1. Обработка персональных данных субъекта, 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).

7.2. Меры по обеспечению безопасности персональных данных субъекта персональных данных при их обработке, осуществляемой без использования средств автоматизации:

7.2.1. Документы, в которых хранятся персональные данные субъекта персональных данных являются документами «Для внутреннего пользования»;

7.2.2. Для хранения таких документов используются специально отведенные помещения и сейфы обеспечивающих защиту от несанкционированного доступа;

7.2.3. Доступ к персональным данным субъекта персональных данных разрешается только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций. Перечень таких лиц утверждается Приказом;

7.3. Мероприятия по обеспечению безопасности персональных данных в Обществе при их обработке в ИСПДн включают в себя:

7.3.1. определение угроз безопасности персональных данных при их обработке;

7.3.2. установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией (перечень программ);

7.3.3. обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

7.3.4. учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

7.3.5. контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

7.3.6. При обнаружении нарушений порядка доступа к персональным данным незамедлительно приостанавливается доступ пользователей к персональным данным, содержащимся в информационной системе до выявления причин нарушений и устранения этих причин.

7.3.7. Работники Общества, осуществляющие обработку персональных данных в ИСПДн, информируются о факте обработки ими персональных данных, категориях обрабатываемых

персональных данных, а также знакомятся под роспись со всей совокупностью требований по обработке и обеспечению безопасности ПДн в части, касающейся их должностных обязанностей.

7.3.8. Запрещены копирование информации, содержащей персональные данные, на съемные флеш-накопители, передача данных по незащищенным каналам связи;

7.3.9. Периодически проводится антивирусный контроль в ИСПДн, к применению в ИСПДн допускаются только лицензированные антивирусные средства.

7.3.10. в ИСПДн запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

7.4. Внешняя защита персональных данных:

7.4.1. Помещения и территория Общества охраняются, в том числе с помощью средств визуального наблюдения.

7.4.2. Персональные данные в зависимости от способа их фиксации (бумажный носитель, электронный носитель) подлежат обработке таким образом, чтобы исключить возможность ознакомления с содержанием указанной информации сторонними лицами.

7.5. Внутренняя защита персональных данных:

7.5.1. Персональные данные, содержащиеся на бумажных носителях.

7.5.2. Персональные данные, содержащиеся на электронных носителях информации, хранятся в памяти персональных компьютеров операторов. Доступ к указанным персональным компьютерам строго ограничен кругом лиц, ответственных за обработку персональных данных.

Информация на электронных носителях должна быть защищена паролем доступа, который подлежит смене не реже 1 (одного) раза в 3 (три) месяцев.

7.6. Приказом устанавливается перечень лиц, имеющих доступ к персональным данным субъекта персональных данных;

7.7. Приказом устанавливается перечень лиц ответственных за реализацию мер обеспечивающих сохранность персональных данных субъекта персональных данных и исключающих несанкционированный доступ к ним.

7.8. При выявлении нарушений в работе с персональными данными, проводится служебная проверка с составлением 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, разработка и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

7.9. Перечень должностей, у которых доступ к персональным данным, обрабатываемым в ИСПДн, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании списка, утвержденного Приказом.

Приложение:

1. Акт об уничтожении персональных данных.

Приложение № 1
к Правилам обработки персональных данных
в ООО «ЖилКомИнкасо-Нижний Новгород»

Ответственный за обеспечение безопасности
персональных данных

" ____ " _____ 20__ г.

Акт
об уничтожении персональных данных

" ____ " _____ 20__ г.

№ _____

Комиссия в составе:

	ФИО	Должность
Председатель:	_____	_____
Сопредседатель:	_____	_____
Члены комиссии:	_____	_____
	_____	_____

провела отбор носителей персональных данных и установила, что в соответствии с требованиями руководящих документов по защите информации _____ информация, записанная на них в процессе эксплуатации, подлежит уничтожению:

№ п/п	Дата	Тип носителя	Регистрационный номер носителя персональных данных	Примечание

Всего подлежит уничтожению _____ носителей
(цифрами и прописью)

После утверждения акта перечисленные носители сверены с записями в акте и на указанных носителях персональные данные уничтожены путем _____

(стирания на устройстве гарантированного уничтожения информации и т.п.)

После утверждения акта перечисленные носители сверены с записями в акте и уничтожены путем _____

(разрезания, сжигания, механического уничтожения, сдачи предприятию по утилизации вторичного сырья и т.п.)

Уничтоженные носители учета персональных данных списаны.

	ФИО	Подпись
Председатель:	_____	_____
Сопредседатель:	_____	_____
Члены комиссии:	_____	_____
	_____	_____