

Положение о защите и порядке обработки персональных данных клиентов

1. Общие положения

1.1. Положение о защите и порядке обработки персональных данных клиентов (далее - Положение) ООО " ЭЙЧ БИ КАПИТАЛ " (далее – Оператор) разработано в соответствии с законодательством Российской Федерации, в том числе Конституцией Российской Федерации, Гражданским кодексом Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом Российской Федерации от 06.04.2011 №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом Российской Федерации от 27.07.2006 №152-ФЗ «О персональных данных», Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», иными нормативно-правовыми актами (далее по тексту – законодательство) и устанавливает порядок работы с персональными данными (далее – ПДн) клиентов (далее - субъектов), обрабатываемыми Оператором.

1.2. Принятие Положения преследует следующие цели:

- защита ПДн субъектов от несанкционированного доступа и разглашения;
- обеспечение защиты прав и свобод субъектов при обработке их ПДн Оператором;
- предотвращение и выявление нарушений законодательства о ПДн, устранение последствий выявленных нарушений;
- установление мер ответственности работников, имеющих допуск и доступ к ПДн субъектов, за невыполнение/нарушение требований законодательства, регулирующего обработку ПДн.

1.3. Все работники Оператора, допущенные к обработке ПДн субъектов, должны быть ознакомлены под роспись с Положением и изменениями к нему.

2. Термины и определения

2.1. Персональные данные субъектов – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн);

2.2. Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн;

2.3. Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн;

2.4. Автоматизированная обработка персональных данных – обработка ПДн с помощью средств вычислительной техники;

2.5. Распространение персональных данных – действия, направленные на раскрытие ПДн неопределенному кругу лиц;

2.6. Предоставление персональных данных – действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц;

2.7. Блокирование персональных данных – временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн);

2.8. Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание ПДн в информационной системе ПДн и (или) в результате которых уничтожаются материальные носители ПДн;

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

2.10. Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий, и технических средств;

2.11. Трансграничная передача персональных данных – передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

2.12. Информация – сведения (сообщения, данные) независимо от формы их представления;

2.13. Документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель.

3. Понятие и состав ПДн субъекта

Полный состав ПДн субъектов, обрабатываемых Оператором, указан в Политике в отношении обработки персональных данных (далее по тексту - Перечень ПДн).

3.1. Информация, содержащая ПДн субъектов, необходима Оператору в целях:

- оказания услуг в соответствии с видами деятельности Оператора;
- оформления и выполнения договорных, преддоговорных отношений;
- выполнения требований законодательства Российской Федерации, регулирующего деятельность юридических лиц;
- защиты законных прав и интересов Оператора;
- обеспечения реализации положений, установленных локальными актами Оператора;
- подготовки, заключения и исполнения гражданско-правового договора.

3.2. Состав и объем ПДн субъектов, необходимый Оператору, устанавливается в зависимости от категории субъекта и обрабатывается в соответствии с целями обработки и положениями соответствующего законодательства.

4. Порядок обработки ПДн субъектов

4.1. Обработка ПДн субъектов должна осуществляться с соблюдением принципов и правил, предусмотренных законодательством.

4.2. Организацию и контроль за порядком обработки и защитой ПДн субъектов в структурных подразделениях Оператора, работники которых обрабатывают ПДн, осуществляют их непосредственные руководители.

4.3. Оператор вправе поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено законодательством, на основании заключаемого с этим лицом договора (контракта). При этом лицо, осуществляющее обработку ПДн по поручению Оператора, обязано соблюдать принципы и правила обработки ПДн, предусмотренные законодательством.

4.4. Уничтожение персональных данных (носителей, содержащих ПДн), производится в соответствии с локальными актами Оператора.

5. Помещения, в которых обрабатываются ПДн субъектов

5.1. ПДн субъектов обрабатываются в структурных подразделениях Оператора по направлениям деятельности. В целях выполнения своих трудовых обязанностей ПДн субъектов могут обрабатываться как на бумажных носителях, так и в электронном виде.

5.2. Помещения, в которых ведется обработка ПДн субъектов, их оборудование должны исключать возможность бесконтрольного проникновения в них посторонних лиц и гарантировать сохранность находящихся в них носителей, содержащих ПДн.

5.3. Помещения, в которых обрабатываются ПДн субъектов, при отсутствии в них работников должны быть заперты.

6. Особенности обработки ПДн без использования средств автоматизации

6.1. ПДн при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях ПДн (далее - материальные носители), в специальных разделах или на полях форм (бланков).

6.2. При фиксации ПДн на материальных носителях не допускается фиксация на одном материальном носителе ПДн, цели обработки которых, заведомо не совместимы. Для обработки различных категорий ПДн, осуществляемой без использования средств автоматизации, для каждой категории ПДн должен использоваться отдельный материальный носитель.

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

- при необходимости использования или распространения определенных ПДн отдельно от находящихся на том же материальном носителе других ПДн осуществляется копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПДн, не подлежащих распространению и использованию, и используется (распространяется) копия ПДн;
- при необходимости уничтожения или блокирования части ПДн уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению или блокированию.

6.4. Уничтожение или обезличивание части ПДн, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание). В таком случае составляется акт, утверждаемый единоличным исполнительным органом (далее – Руководителем).

6.5. Уточнение ПДн 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 ПДн.

6.6. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются Оператором.

6.7. При работе с материальными носителями, содержащими ПДн, работники Оператора должны исключить несанкционированный к ним доступ, соблюдая следующие правила:

- при угрозе несанкционированного доступа к материальным носителям, содержащим ПДн, работник обязан исключить возможность визуального съема информации с них и убрать носитель(и) в запираемый шкаф (сейф и т.п.);
- покидая рабочее место, все материальные носители, содержащие ПДн, должны убираться в запираемый шкаф (сейф и т.п.);
- работник обязан принимать иные меры в соответствии со сложившейся ситуацией, исходя из обязанности исключения несанкционированного доступа к материальным носителям, содержащим ПДн.

6.8. Работники, осуществляющие обработку ПДн без использования средств автоматизации, должны быть проинформированы о факте обработки ими ПДн, категориях обрабатываемых ПДн, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами Оператора.

7. Особенности обработки ПДн в ИСПДн

7.1. Оператор при обработке ПДн в ИСПДн обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении ПДн.

7.2. Порядок обработки ПДн в ИСПДн Оператора регламентируется Положением и иными локальными нормативными актами Оператора в области технической защиты ПДн.

7.3. Допуск к обработке ПДн в ИСПДн имеют работники согласно приказу об утверждении перечня должностей работников, доступ которых к персональным данным, необходим для выполнения трудовых обязанностей, утвержденному Руководителем. Доступ работников в ИСПДн реализуется посредством технических средств и способов, не противоречащих законодательству Российской Федерации.

7.4. Использование средств вычислительной техники для обработки ПДн в ИСПДн допускается только после выполнения требований безопасности информации.

7.5. Обеспечение безопасности ПДн достигается, в частности:

- определением угроз безопасности ПДн при их обработке в ИСПДн;
- применением организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности ПДн;
- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- оценкой эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;
- учетом машинных носителей ПДн;
- обнаружением фактов несанкционированного доступа к ПДн и принятием соответствующих мер;
- восстановлением ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установлением правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечением регистрации и учета всех действий, совершаемых с ПДн в ИСПДн;
- контролем за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ИСПДн.

7.6. При проведении технического обслуживания и ремонта техники, в которой ведется обработка ПДн, запрещается передавать ремонтным организациям блоки с элементами накопления и хранения ПДн.

7.7. Машинные носители, содержащие ПДн (несъемные диски - жесткие диски; съемные носители: гибкие магнитные диски, съемные пакеты дисков, иные магнитные, оптические или магнитно-оптические диски и т.п.) до начала работы регистрируются администратором информационной безопасности с проставлением реквизитов, идентифицирующих каждый носитель.

7.8. Доступ работников в ИСПДн реализуется посредством технических средств и способов, не противоречащих законодательству Российской Федерации.

7.9. Работники, обрабатывающие ПДн в ИСПДн, обязаны соблюдать следующие требования:

- проверять все новые данные на наличие вирусов;
- никому не сообщать (не передавать) сведения о доступе (логин, пароль);
- не оставлять без контроля включенным автоматизированное рабочее место;
- при оставлении рабочего места программное обеспечение, используемое при обработке ПДн в ИСПДн, переводится в режим работы, исключающий доступ к информации без ввода пароля или идентификатора.

7.10. Оператор производит регулярное резервное копирование данных в ИСПДн.

7.11. Оператор обязан в порядке, определенном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование его о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных.

8. Права и обязанности субъектов

8.1. Субъект ПДн имеет право:

- на получение сведений, указанных в п. 8.2. Положения, за исключением случаев, когда право субъекта на доступ к его ПДн ограничено в соответствии с федеральными законами;
- требовать от Оператора уточнения своих ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;
- при обращении или направлении запроса требовать от Оператора предоставления сведений о наличии его ПДн в доступной форме. При этом в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн.

8.2. Запрос должен отвечать требованиям пункта 3 статьи 14 Федерального закона Российской Федерации от 27.07.2006 №152-ФЗ «О персональных данных». При этом подлежит предоставлению следующая информация:

- подтверждение факта обработки ПДн субъекта Оператором;
- правовые основания и цели обработки ПДн;
- цели и применяемые способы обработки ПДн;
- наименование и место нахождения Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Оператором или на основании федерального закона;
- обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок предоставления таких данных не предусмотрен федеральным законом;
- сроки обработки ПДн, в том числе сроки их хранения;
- порядок осуществления субъектом ПДн прав, предусмотренных Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных»;
- информацию об осуществляемой или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Оператора, если обработка поручена или будет поручена такому лицу;

- информацию о способах исполнения оператором обязанностей, установленных статьей 18.1 настоящего Федерального закона;
- иные сведения, предусмотренные Федеральным законом Российской Федерации от 27.07.2006 №152-ФЗ «О персональных данных» или другими федеральными законами.

Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

8.3. Оператор предоставляет вышеуказанные сведения субъекту персональных данных или его представителю в той форме, в которой направлены соответствующие обращение либо запрос, если иное не указано в обращении или запросе.

8.4. После предоставления необходимых сведений субъекту ПДн по его запросу, последний вправе обратиться повторно к Оператору или направить ему повторный запрос о предоставлении данных, не ранее чем через 30 дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен законодательством, нормативно-правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн.

8.5. Субъект ПДн вправе обратиться повторно к Оператору или направить ему повторный запрос в целях получения необходимых сведений, а также в целях ознакомления с обрабатываемыми ПДн до истечения срока, указанного в п. 8.4. Положения в случае, если такие сведения и (или) обрабатываемые ПДн не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения.

Повторный запрос наряду со сведениями, предусмотренными законодательством, должен содержать обоснование его направления.

8.6. Оператор вправе отказать субъекту ПДн в выполнении повторного запроса, не соответствующего условиям, предусмотренным законодательством. Такой отказ должен быть мотивированным. Обязанность предоставления доказательств обоснованности отказа в выполнении повторного запроса лежит на Операторе.

9. Обеспечение конфиденциальности и защиты ПДн

9.1. К информации, содержащей ПДн субъектов, применяется режим конфиденциальности, то есть обязательное для соблюдения получившим доступ к ПДн субъектов лицом требование не раскрывать третьим лицам и не допускать их распространения без согласия субъекта ПДн или иного законного основания.

9.2. Оператор при обработке ПДн принимает необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении ПДн.

9.3. Защита ПДн направлена на предупреждение нарушения порядка доступа к ПДн, обеспечение сохранности носителей, содержащих ПДн, обеспечение достоверности ПДн и соблюдение режима конфиденциальности ПДн.

9.4. Конфиденциальность и защита ПДн обеспечиваются путем принятия Оператором следующих мер:

- определение перечня ПДн субъектов, обрабатываемых Оператором;
- ограничение доступа к ПДн путем определения должностных лиц, допущенных к обработке ПДн;
- определение работников, ответственных за: организацию обработки ПДн; реализацию мер, необходимых для обеспечения условий для сохранности персональных данных и исключения несанкционированного к ним доступа; обеспечение безопасности ПДн в информационной системе; распределение между ними соответствующих обязанностей;
- регламентация правил обработки ПДн субъектов путем установления порядка работы с этой информацией и контроля за его соблюдением;

- учет лиц, получивших доступ к ПДн субъектов, и (или) лиц, которым такая информация была предоставлена или передана;
- регулирование отношений по использованию ПДн субъектов в рамках договорных отношений;
- выявление возможных каналов несанкционированного доступа к ПДн субъектов, обеспечение безопасности информации при обработке ПДн субъектов с использованием средств вычислительной техники;
- исключение бесконтрольного использования средств обработки ПДн субъектов посторонними лицами;
- определение помещений, в которых ведется работа с ПДн субъектов, исключение бесконтрольного доступа посторонних лиц в эти помещения;
- определение мест обработки (хранения) материальных носителей, содержащих ПДн;
- использование необходимых средств технической защиты информации в ИСПДн;
- организация надлежащего порядка уничтожения ПДн, их материальных носителей;
- своевременное выявление нарушения требований разрешительной системы доступа работниками к определенным сведениям;
- проведение воспитательной и разъяснительной работы с работниками по предупреждению нарушения норм законодательства, регулирующего обработку ПДн, обучение;
- принятие иных мер, не противоречащих законодательству.

9.5. Право доступа к ПДн имеют работники, занимающие соответствующие должности, утвержденные Руководителем.

Работники Оператора обрабатывают ПДн только в том объеме, который необходим им для выполнения своих трудовых обязанностей.

9.6. При обработке ПДн работники должны обеспечивать безопасность носителей, содержащих ПДн, находящихся в их распоряжении.

9.7. Работники, обрабатывающие ПДн, обязаны обеспечивать их конфиденциальность, соблюдать требования законодательства, настоящего Положения и иных локальных актов Оператора, обеспечивать защиту ПДн от несанкционированного доступа.

9.8. Работникам, осуществляющим обработку ПДн, запрещается оставлять вне контроля материальные носители и средства обработки ПДн. При оставлении рабочего места материальные носители убираются в запираемые шкафы, сейфы и т.п., а программное обеспечение, используемое при обработке ПДн в ИСПДн, переводится в режим работы, исключающий доступ к информации без ввода пароля или идентификатора.

10. Служебное расследование по фактам нарушения режима конфиденциальности и правил обработки ПДн.

10.1. За нарушение правил обработки ПДн виновные лица привлекаются к ответственности в соответствии с законодательством.

10.2. По факту нарушения правил обработки ПДн может быть организовано служебное расследование.

10.3. Для проведения расследования Оператор образует комиссию. Основная задача комиссии - правильное и объективное установление всех обстоятельств, а также сбор и анализ доказательной базы.

10.4. В процессе проверочных мероприятий комиссия обязана:

- установить факт совершения дисциплинарного проступка, обстоятельства его совершения;
- при утере носителя(ей) провести обследование мест возможного нахождения утерянного(ых) носителя(ей), содержащего(их) ПДн;
- определить вину лиц, допустивших нарушение правил обработки ПДн (разглашение ПДн либо утерю носителя(ей), содержащего(их) ПДн);

- определить размер причиненного Оператору ущерба;
- выявить мотивы и причины совершения проступка, а также смягчающие и отягчающие обстоятельства;
- соблюдать требования законодательства в части защиты неприкосновенности личной информации работников;
- не придавать огласке информацию, касающуюся проверки.

10.5. При проведении проверочных мероприятий члены комиссии имеют право:

- проводить анализ документации, касающейся обработки ПДн Оператором;
- запросить письменные объяснения от сотрудника(ов), в отношении которого(ых) проводится проверка, об обстоятельствах произошедшего; если по истечении двух рабочих дней они не представлены - составить соответствующий акт;
- получать письменные пояснения от работников Оператора;
- проводить осмотр помещений, хранилищ, столов, шкафов, в которых может(гут) находиться носитель(и), содержащие ПДн (в случае утери);
- направлять запросы в адрес контрагентов, а также в органы государственной власти и местного самоуправления, организации.

10.6. По результатам работы комиссии Руководитель в случае виновности работника(ов) вправе применить в отношении него(них) одно из дисциплинарных взысканий. Взыскание не может быть применено позднее шести месяцев со дня совершения проступка и позднее одного месяца со дня его обнаружения.

11. Ответственность за нарушение норм, регулирующих обработку и защиту ПДн

11.1. Работник, обрабатывающий ПДн, несет ответственность за нарушение установленного порядка и правил обработки.

11.2. Руководитель подразделения осуществляет контроль за обработкой ПДн работниками в своем подразделении.

11.3. В случае нарушения норм, регулирующих обработку и защиту ПДн, работник может быть:

- привлечен к дисциплинарной и материальной ответственности в порядке, установленном трудовым кодексом Российской Федерации и иными федеральными законами;
- привлечен к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

12. Проведение внутреннего контроля и (или) аудита соответствия обработки ПДн законодательству, требованиям к защите ПДн, политике Оператора в отношении обработки ПДн, локальным актам

12.1. Внутренний контроль и (или) аудит соответствия обработки ПДн законодательству о ПДн, требованиям к защите ПДн, политике Оператора в отношении обработки ПДн, локальным актам, осуществляется с целью изучения и оценки фактического состояния соблюдения правил обработки ПДн, обеспечения надлежащей защиты ПДн, выявления недостатков и нарушений, выработки предложений, направленных на их устранение и предотвращение.

12.2. Контрольные мероприятия проводятся ответственным за организацию обработки ПДн, Оператором либо образуемой комиссией из числа работников, имеющих допуск к ПДн, Руководителем согласно утвержденному ежегодному плану в соответствии с Правилам проведения внутреннего контроля в отношении обработки персональных данных. При необходимости, может быть проведена внеплановая проверка.

Проведение проверки не должно приводить к необоснованному ознакомлению с ПДн участвующих в ней лиц.

12.3. По результатам проверки составляется отчет с отражением в нем состояния дел Оператора, по соблюдению требований законодательства, регламентирующего обработку ПДн, выявленных недостатков и нарушений правил обработки ПДн, предложений по их устранению.

12.4. Отчет предоставляет Руководитель. На основании представленного отчета Руководитель определяет ответственных работников и сроки устранения выявленных нарушений, недостатков, принимает иные необходимые решения.

13. Заключительные положения

13.1. Настоящее Положение вступает в силу с момента его утверждения и действует бессрочно до замены его новым.

13.2. Настоящее Положение обязательно для всех работников Оператора.

13.3. Все работники Оператора должны быть ознакомлены под подпись с данным Положением и изменениями к нему.

31.07.2025 г.

Генеральный директор
ООО "ЭЙЧ БИ КАПИТАЛ "


 /Скочко В.В.