Приложение к Приказу ООО «КИВИ Блокчейн Технологии» №4/1 от 13 июня 2018г.

Утверждено
Генеральный директор ООО «КИВИ Блокчейн Технологии»

_____ / Я.А. Баринский /

ПОЛОЖЕНИЕ

об обработке персональных данных
в Обществе с ограниченной ответственность «КИВИ Блокчейн Технологии»

1 Общие положения

1.1. Назначение документа

1.1.1 Настоящее Положение определяет порядок и условия обработки персональных данных (далее – ПДн) в ООО «КИВИ Блокчейн Технологии» (далее – Компания), включая следующее:

- организационная структура обработки и обеспечения безопасности ПДн;
- порядок и условия обработки ПДн;
- порядок взаимодействия с государственными органами по вопросам обработки и обеспечения безопасности ПДн;
- порядок организации внутреннего контроля обработки ПДн;
- ответственность за нарушение порядка и условий обработки ПДн.

1.1.2 Настоящее Положение предназначено для организации в Компании процесса обработки ПДн согласно нормам и принципам действующего федерального законодательства.

1.2. Область действия

1.2.1 Действие настоящего Положения распространяется на все процессы по сбору, записи, систематизации, накоплению, хранению, уточнению (обновлению и изменению), извлечению, использованию, передаче (распространению, предоставлению, доступу), обезличиванию, блокированию, удалению, уничтожению ПДн, осуществляемых с использованием средств автоматизации и без их использования.

1.2.2 Действие настоящего Положения распространяется на все информационные системы ПДн Компании (далее – ИСПДн).

1.2.3 Положение обязательно для ознакомления и исполнения всем лицами, допущенным к обработке ПДн.

1.2.4 Положение по обработке персональных данных работников определено в Приложение 8.

1.3. Нормативно-правовая основа

1.3.1 Настоящее Положение разработано в соответствии с законодательством Российской Федерации о ПДн и нормативно-методическими документами исполнительных органов государственной власти по вопросам безопасности ПДн.

1.3.2 Нормативные правовые и методические документы, на которых основывается настоящее Положение:

- Федеральный Закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»;

- «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденные Постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119;
- Приказ ФСТЭК «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при обработке в информационных системах персональных данных» от 18.02.2013 года № 21.
- «Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденное Постановлением Правительства Российской Федерации от 15.09.2008 г. № 687.

2 Организационная структура обработки и обеспечения безопасности ПДн

2.1. Должностное лицо, ответственное за организацию обработки ПДн

2.1.1. В Компании назначено Должностное лицо, ответственное за организацию обработки ПДн, на которое возложено выполнение следующих задач:

- организация работ по выполнению требований законодательных и нормативных документов Российской Федерации в области обработки и обеспечения безопасности ПДн;
- контроль выполнения требований законодательных и нормативных документов Российской Федерации в области обработки и обеспечения безопасности ПДн, а также настоящего Положения;
- взаимодействие с регулирующими органами по вопросам обработки и обеспечения безопасности ПДн;
- организация процесса передачи ПДн и поручения обработки ПДн в соответствии с требованиями законодательных и нормативных документов Российской Федерации в области обработки и обеспечения безопасности ПДн;
- устранение нарушений при обработке ПДн в Компании и уведомление субъектов ПДн, в отношении ПДн которого допущены нарушения, и/или регулирующих органов об устранении таких нарушений.

2.1.2. Должностное лицо, ответственное за организацию обработки ПДн, обязано руководствоваться в своей работе законодательными и нормативными документами в области обеспечения безопасности ПДн в Российской Федерации, а также настоящим Положением и другими актами Компании, регламентирующими защиту ПДн.

2.1.3. В Компании назначено Должностное лицо, ответственное за безопасность ПДн, на которое возложено выполнение следующих задач:

- осуществление выбора и реализации методов и способов защиты информации, применяемых для обеспечения безопасности персональных данных при их обработке в ИСПДн;
- организация работ по формированию и пересмотру моделей угроз безопасности персональных данных при их обработке в информационных системах ПДн Компании;
- организация работ по созданию системы защиты персональных данных (комплекса организационно-технических мер), обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса информационных систем;
- контроль выполнения мероприятий по защите ПДн и обеспечение работоспособности системы защиты ПДн, реализуемых в рамках подсистем защиты с учетом класса информационной системы;
- контроль соответствия эксплуатации информационных систем ПДн требованиям организационно-технической и эксплуатационной документации;
- контроль соблюдения работниками Компании установленных требований по обеспечению безопасности ПДн;
- разработка предложений по совершенствованию системы защиты ПДн;
- эксплуатация ИСПДн в соответствии с организационно-технической и эксплуатационной документацией;

- организация мероприятий по восстановлению ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- учет, установка и ввод в эксплуатацию (проведение работ, связанных с монтажом, настройкой и проверкой работоспособности) средств защиты информации в соответствии с эксплуатационной и технической документацией.
- проверка готовности средств защиты информации к использованию;
- реализация предложений по совершенствованию системы защиты ПДн;
- организация обучения лиц применяющих средства защиты информации, правилам работы с ними;
- организация работ по подготовке объектов информатизации (в том числе информационных систем персональных данных) к оценке соответствия по требованиям безопасности информации;
- проверка выполнения требований к помещениям, в которых производится обработка ПДн;
- контроль порядка и своевременности блокирования учётных записей пользователей при изменении штатной структуры (увольнении, перемещении работников).

2.2. Структурные подразделения Компании

2.2.1. Работники Структурных подразделений Компании выполняют следующие задачи при осуществлении обработки ПДн, которые стали им известны в период исполнения служебных обязанностей:

- осуществление взаимодействия с субъектами ПДн (или их законными представителями) по вопросам сбора (получения) их ПДн, в т.ч. разъяснение субъекту ПДн юридических последствия отказа предоставить его ПДн; по вопросам получения необходимых согласий на обработку и передачу их ПДн; уточнения, блокирования или уничтожения их ПДн; по вопросам предоставления им необходимых сведений; по вопросам дачи им уведомлений и разъяснений; по вопросам их запросов и обращений.
- осуществление взаимодействия с третьими лицами по вопросам передачи и поручения обработки ПДн;
- участие (в случае необходимости) в расследовании инцидентов, связанных с нарушением условий и принципов обработки ПДн и безопасности ПДн;
- обеспечение конфиденциальности и целевого использования ПДн.

2.2.2. Работники Компании, осуществляющие обработку ПДн, обязаны руководствоваться в своей работе законодательными и нормативными документами Российской Федерации в области ПДн, а также настоящим Положением и другими актами Компании, регламентирующими защиту ПДн.

2 Порядок передачи персональных данных

2.1. В Компании может осуществляться трансграничная передача ПДн субъектов. В случае необходимости трансграничной передачи с субъекта ПДн берется письменное согласие.

2.2. В соответствии с требованиями ч. 1 ст. 6 ФЗ «О персональных данных» обработка ПДн с их передачей в ИСПДн, принадлежащие сторонним организациям (третьим лицам), допускается в случае наличия согласия субъекта ПДн (п. 1 ч. 1 ст. 6 ФЗ «О персональных данных»). В этих целях Компания запрашивает согласие субъектов ПДн на передачу ПДн.

2.3. Перечень третьих лиц, которым передаются ПДн субъектов, указываются в подписываемом субъектом согласии на обработку.

2.4. В случае заключения договора с новым контрагентом (обработчиком), в рамках которого предполагается передача ПДн, необходимо соблюдение двух обязательных условий:

- наличия согласия субъекта ПДн по форме на передачу ПДн, приведенной в Приложении 2;
- заключения с юридическим лицом поручения на обработку ПДн по форме, приведенной в Приложении 1.

2.5. Передача ПДн внутри Компании осуществляется только между работниками, имеющими доступ к ПДн соответствующей категории субъектов ПДн.

2.6. Работники Компании, передающие ПДн третьим лицам, должны передавать их с обязательным уведомлением лица, получающего эти данные, об обязанности использования полученной информации лишь в целях, для которых она была передана, и с предупреждением об ответственности за незаконное использование данной информации в соответствии с федеральными законами.

2.7. Законному представителю субъекта ПДн данные соответствующего субъекта ПДн передаются в порядке, установленном законодательством Российской Федерации, информация передается при наличии документов, подтверждающих полномочия представителя.

2.8. Предоставление ПДн государственным органам производится в соответствии с требованиями законодательства Российской Федерации.

2.9. ПДн могут быть предоставлены родственникам или членам семьи субъекта ПДн (кроме законных представителей) только с письменного разрешения самого субъекта ПДн, за исключением случаев, когда передача ПДн без его согласия допускается законодательством Российской Федерации.

2.10. Учет переданных ПДн по запросам осуществляется в рамках принятых в Компании правил делопроизводства путем регистрации входящей и исходящей корреспонденции и запросов субъектов ПДн, государственных органов, иных лиц и структурных подразделений Компании о предоставлении ПДн. При регистрации фиксируются сведения о лицах, направивших такие запросы, дата выдачи (предоставления доступа) ПДн, направления ответа на запрос либо дата уведомления об отказе в предоставлении ПДн (в случае отказа).

2.11. В случае, если лицо, обратившееся в Компанию с запросом на предоставление ПДн, не уполномочено на получение информации, относящейся к ПДн, Компания обязана отказать лицу в выдаче такой информации. Лицу, обратившемуся с соответствующим запросом, выдается уведомление в свободной форме об отказе в выдаче информации, а копия уведомления хранится в соответствии с принятыми правилами делопроизводства (как исходящая корреспонденция).

3 Уничтожение персональных данных

3.1. ПДн субъектов подлежат уничтожению, если иное не предусмотрено федеральными законами или соглашением между Компанией и субъектом ПДн, в следующих случаях:

- по требованию субъекта ПДн или уполномоченного органа по защите прав субъектов ПДн, если ПДн являются неполными, устаревшими, недостоверными, полученными незаконно или не являются необходимыми для заявленной цели обработки;
- в случае отзыва субъектом ПДн согласия на обработку своих ПДн (если дальнейшая обработка ПДн не требуется в соответствии с требованиями законодательства);
- в случае выявления неправомерной обработки ПДн и невозможности устранения допущенных нарушений;
- по достижении целей обработки или в случае утраты необходимости в их достижении.

3.2. ПДн должны быть уничтожены на всех носителях, в т.ч. внешних/съемных электронных носителях, бумажных носителях и в ИСПДн, в которых они обрабатываются.

3.3. Ответственный за организацию обработки ПДн сообщает руководителям структурных подразделений Компании, в которых обрабатываются ПДн указанного субъекта, о необходимости уничтожения ПДн конкретного субъекта при поступлении соответствующих запросов.

3.4. Ежеквартально Ответственный за организацию обработки ПДн в Компании инициирует процесс уничтожения ПДн, цели обработки которых были достигнуты.

3.5. Уничтожение ПДн может проводиться путем уничтожения ПДн с носителя, без возможности последующего восстановления, либо путем уничтожения непосредственно материального носителя.

3.6. Уничтожение ПДн в ИСПДн осуществляется работниками Департамента эксплуатации информационных систем или Департамента автоматизации финансового учета и отчетности, Дирекции безопасности с использованием внутренних средств ИСПДн.

3.7. Уничтожение бумажных носителей ПДн осуществляется Отделом документационного обеспечения, отделом кадров, Дирекцией по работе с персоналом путем измельчения при помощи уничтожителя бумаг – шредера.

3.8. Уничтожение ПДн на электронных носителях может проводиться с помощью специализированного ПО для удаления файлов.

3.9. Уничтожение ПДн путем физического уничтожения электронного носителя производится при помощи раздробления или размагничивания носителя.

3.10. Если уничтожение части ПДн допускается носителем, то уничтожение производится способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на данном материальном носителе (удаление, вымарывание).

3.11. Если уничтожение части ПДн носителем не допускается, то сведения, не подлежащие уничтожению, копируются способом, исключающим одновременное копирование ПДн, подлежащих уничтожению, а материальный носитель уничтожается.

3.12. По результатам уничтожения персональных данных должен оформляться Акт об уничтожении персональных данных (форма акта приведена в Приложение 3). При уничтожении ПДн путем физического уничтожения машинного носителя также должны проставляться отметки в учетных формах, имеющихся в Компании.

4 Общие требования к обработке персональных данных

4.1. В Компании обрабатываются ПДн, принадлежащие клиентам, контрагентам, их представителям и контактным лицам; кадидатам; участникам маркетинговых исследований; работникам Компании и родственникам работников; кандидатам на замещение вакантных должностей в Компании; лицам, являющимся стороной договора гражданско-правового характера; директорам, акционерам, учредителям, супругам акционеров, наследникам акционеров, членам Совета директоров Компании; аффилированным лицам Компании и лицам, входящим в одну группу с Компанией, лицам, проходящим по судебным делам с участием Компании; поручителям по коммерческим кредитам; лицам, которым осуществляется курьерская доставка; получателям алиментов от работников Компании (далее – ПДн субъектов).

4.1.1. Цели обработки ПДн субъектов определены в документе «Политика в отношении обработки персональных данных ООО «КИВИ Блокчейн Технологии».

4.1.2. ПДн субъектов обрабатываются в составе и сроки на основании требований законодательства Российской Федерации.

4.1.3. Обработка ПДн осуществляется только после того, как субъект дал свое согласие на обработку своих ПДн, за исключением случаев, предусмотренных действующим законодательством РФ:

Согласие на обработку ПДн родственников *не требуется* в связи с тем, что обработка их ПДн необходима для исполнения требований трудового законодательства РФ.

Согласие на обработку ПДн контрагентов, их представителей и контактных лиц контрагентов *не требуется* в связи с тем, что обработка их ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн, а также в связи с тем, что обработка ПДн необходима для достижения целей, предусмотренных законом Российской Федерации и осуществления и выполнения возложенных законодательством Российской Федерации на Компанию функций, полномочий и обязанностей.

Согласие на обработку ПДн участников маркетинговых исследований *не требуется* в связи с тем, что обработка ПДн осуществляется в статистических или иных исследовательских целях, при условии обязательного обезличивания персональных данных.

Согласие на обработку ПДн лиц, являющихся стороной договора гражданско-правового характера, *не требуется* в связи с тем, что обработка их ПДн необходима для исполнения договора, стороной которого по которому является субъект ПДн, а также в связи с тем, что обработка ПДн необходима для достижения целей, предусмотренных законом Российской Федерации и осуществления и выполнения возложенных законодательством Российской Федерации на Компанию функций, полномочий и обязанностей.

Согласие на обработку ПДн директоров, акционеров, учредителей, супругов акционеров, наследников акционеров, членов Совета директоров Компании *не требуется* в связи с тем, что обработка их ПДн необходима для достижения целей, предусмотренных законом Российской Федерации и осуществления и выполнения возложенных законодательством Российской Федерации на Компанию функций, полномочий и обязанностей.

Согласие на обработку ПДн аффилированных лиц Компании и лиц, входящих в одну группу с Компанией, *не требуется* в связи с тем, что обработка их ПДн необходима для достижения целей, предусмотренных законом Российской Федерации и осуществления и выполнения возложенных законодательством Российской Федерации на Компанию функций, полномочий и обязанностей.

Согласие на обработку ПДн лиц, проходящих по судебным делам с участием Компании, *не требуется* в связи с тем, что обработка их ПДн необходима для осуществления прав и законных интересов Компании или третьих лиц, с соблюдением условия, что при этом не нарушаются права и свободы субъекта ПДн. Обработка их ПДн необходима для правового обеспечения и обеспечения законности деятельности Компании, защиты законных прав и интересов компании.

Согласие на обработку ПДн поручителей по коммерческим кредитам *не требуется* в связи с тем, что обработка их ПДн необходима для исполнения договора, поручителем по которому является субъект ПДн.

Согласие на обработку ПДн лиц, которым осуществляется курьерская доставка, *не требуется в связи с тем, что обработка ПДн* необходима для осуществления прав и законных интересов Компании или третьих лиц, с соблюдением условия, что при этом не нарушаются права и свободы субъекта ПДн .

Согласие на обработку ПДн получателей алиментов *не требуется* в связи с тем, что обработка их ПДн необходима для достижения целей, предусмотренных законом Российской Федерации и осуществления и выполнения возложенных законодательством Российской Федерации на Компанию функций, полномочий и обязанностей, а также для исполнения судебного акта.

4.2. Предоставление ПДн субъектов является обязательным в соответствии с федеральным законом, в связи с чем Компания обязана разъяснить субъекту юридические последствия отказа предоставить их ПДн.

4.3. ПДн субъектов обрабатываются в Компании в ИСПДн, при этом:

- не допускается объединения баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой;
- хранение ПДн осуществляется таким образом, что в отношении каждой категории ПДн можно определить места их хранения;
- хранение ПДн осуществляется в такой форме, которая позволит определить субъекта ПДн, но не дольше, чем этого требуют цели обработки ПДн или согласие субъекта ПДн;
- несанкционированный доступ к ПДн исключен.

4.4. ПДн субъектов могут обрабатываться в Компании без использования средств автоматизации, при этом:

- ПДн обособляются от иной информации;
- не допускается фиксация на одном материальном носителе ПДн, цели обработки которых заведомо несовместимы.

4.5. Порядок обработки ПДн без средств автоматизации определяется документом «Правила осуществления обработки персональных данных без использования средств автоматизации».

4.6. По запросу субъекта ПДн Компания обязана предоставлять ему необходимую информацию, касающуюся обработки и защиты персональных данных.

4.7. Компания рассматривает запросы и обращения субъектов по вопросам обработки их ПДн в Компании. Компания обязана сообщить субъекту ПДн или его законному представителю информацию, касающуюся обработки его ПДн в течение 30 рабочих дней с момента получения соответствующего запроса. По фактам обращений субъектов в Компанию ведется учет обращений субъектов ПДн. Инструкция по заполнению журнала приведена в Приложении 4.

4.8. ПДн субъектов передаются в органы государственной власти в рамках исполнения Компанией требований федерального законодательства, при этом:

- несанкционированный доступ к ПДн в процессе передачи исключается;
- Компания ограничивается передачей только тех ПДн, которые необходимы для выполнения требований федерального законодательства.

4.9. Уточнение (изменение) неполных, устаревших или неточных ПДн субъектов осуществляется на основании документов, представленных субъектом ПДн или его законным представителем либо уполномоченным органом по защите прав субъектов ПДн. В случае выявления недостоверных ПДн в течение 1 рабочего дня осуществляется блокирование ПДн, относящихся к соответствующему субъекту ПДн, с момента обнаружения таких нарушений на период проверки (уточнения). В случае уточнения (изменения) ПДн Компания по возможности извещает всех лиц, которым ранее были сообщены или переданы неверные или неполные ПДн, обо всех исключениях, исправлениях и дополнениях в них. Уточнение ПДн субъектов при осуществлении их обработки без использования средств автоматизации производится путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными ПДн.

4.10. Полный перечень ПДн, срок, основание обработки детализировано в отдельной форме «Перечень персональных данных, обрабатываемых в информационных системах персональных данных и без использования средств автоматизации» (Приложение 5).

5 Правила доступа к ПДн

5.1. Работники Компании, доступ которых к ПДн, обрабатываемым в Компании, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим ПДн на основании документа «Порядок предоставления доступа к активам ООО «КИВИ Блокчейн Технологии».

5.2. Работникам Компании предоставляется доступ к работе с ПДн исключительно в пределах и объеме, необходимых для выполнения ими своих должностных обязанностей.

5.3. Объем ПДн, необходимых для выполнения работниками своих должностных обязанностей, определяется руководителями Структурных подразделений Компании.

5.4. Работники Компании, которые в силу выполняемых служебных обязанностей постоянно работают с ПДн, получают допуск к необходимым категориям ПДн, с установленными правами доступа, на срок выполнения ими соответствующих должностных обязанностей.

5.5. Список работников, допущенных к работе с ПДн, для каждой ИСПДн должен поддерживаться в актуальном состоянии. С этой целью Список работников, допущенных к работе с ПДн, актуализируется путем анализа категорий работников, которым необходим доступ к ИСПДн руководителями Структурных подразделений Компании. Форма Списка работников, допущенных к работе с ПДн, приведена в Приложении 6.

5.6. Доступ к ПДн может быть прекращен или ограничен в случае:

- нарушения порядка и условий обработки ПДн, установленных в Компании;
- нарушения безопасности ПДн, обрабатываемых в Компании;
- изменения должностных обязанностей, увольнения работника Компании или прекращения договорных отношений с работником Компании.

5.7. Все работники Компании, имеющие действующие трудовые отношения, деятельность которых связана с обработкой и защитой конфиденциальной информацией, в том числе с ПДн, обязаны подписать Соглашение о неразглашении конфиденциальной информации.

6 Порядок взаимодействия с регулирующими органами по вопросам обработки ПДн

6.1. Контроль и надзор за выполнением требований по обработке ПДн в ИСПДн, установленных Правительством Российской Федерации, осуществляются Федеральной службой безопасности[1], и Федеральной службой по техническому и экспортному контролю России[2] в пределах их компетенции и без права ознакомления с ПДн, обрабатываемыми в ИСПДн Компании.

6.2. Компания обязана уведомить уполномоченный орган по защите прав субъектов ПДн[3] о своем намерении осуществлять обработку ПДн (об обработке ПДн).

6.3. Компания обязана сообщить в уполномоченный орган по защите прав субъектов ПДн по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение 30 рабочих дней с даты получения запроса.

6.4. Об устранении допущенных нарушений или об уничтожении ПДн в случае, если обращение субъекта ПДн или его представителя либо запрос уполномоченного органа по защите прав субъектов ПДн были направлены уполномоченным органом по защите прав субъектов ПДн, Компания обязана уведомить указанный орган.

6.5. В установленных федеральным законодательством случаях Компания обязана предоставлять информацию, содержащую обрабатываемые ПДн, по мотивированному запросу уполномоченных органов государственной власти по вопросам их компетенции.

6.6. Запросы на предоставление доступа к обрабатываемым ПДн могут быть обжалованы в судебном порядке в соответствии с законодательством Российской Федерации.

7 Мероприятия по обеспечению безопасности ПДн

7.1. ПДн, обрабатываемые в Компании, являются конфиденциальной информацией, в связи с чем безопасность обрабатываемых в Компании ПДн обеспечивается в соответствии с установленным в Компании порядком защиты конфиденциальной информации.

8 Организация внутреннего контроля обработки и обеспечения безопасности ПДн

8.1. Цели организации внутреннего контроля

8.2.1. Организация внутреннего контроля процесса обработки ПДн в Компании осуществляется в целях своевременного реагирования на нарушения установленного порядка их обработки, а также в целях совершенствования этого порядка и обеспечения его соблюдения.

8.2.2. Мероприятия по осуществлению внутреннего контроля обработки ПДн направлены на решение следующих задач:

- обеспечение соблюдения работниками Компании требований настоящего Положения и нормативных правовых актов Российской Федерации о ПДн;
- выявление нарушений установленного порядка обработки ПДн и своевременное предотвращение негативных последствий таких нарушений;
- принятие корректирующих мер, направленных на устранение выявленных нарушений в порядке обработки ПДн;
- разработка и контроль исполнения рекомендаций по совершенствованию порядка обработки ПДн по результатам контрольных мероприятий.

8.2. Проведение внутреннего контроля

8.2.1. Компания организует проведение внутреннего контроля обработки ПДн.

8.2.2. Ответственным за проведение внутреннего контроля обработки ПДн является должностное лицо, ответственное за организацию обработки ПДн.

8.2.3. Проведение контрольных мероприятий должно включать проведение следующих проверок:

- деятельности работников Компании, допущенных к работе с ПДн, на соответствие порядку обработки и обеспечения безопасности ПДн, установленному настоящим Положением и нормативными правовыми актами Российской Федерации в области персональных данных;
- отслеживание и учет изменений законодательства в области ПДн;

---

1) ФСБ России
2) ФСТЭК России
3) Роскомнадзор

- контроль изменений в процессах обработки ПДн в Компании в части состава обрабатываемых ПДн, появления новых категорий субъектов ПДн, сроков их обработки;
- контроль изменений в процессах обработки ПДн в Компании в части взаимодействия с третьими лицами по вопросам получения и передачи ПДн;
- контроль изменений в ИСПДн Компании.

8.2.4. По результатам проведения контрольных мероприятий производится оценка состояния порядка и условий обработки ПДн в Компании.

8.2.5. В случае обнаружения нарушений порядка и условий обработки ПДн, установленных в Компании, предоставление ПДн пользователям информационных систем ПДн прекращается до устранения нарушений.

8.2.6. Детальная организация внутреннего контроля приведена в Приложении 7.

9 Ответственность за нарушения при обработке ПДн

9.1. Руководство Компании несет ответственность за обеспечение конфиденциальности, целостности и доступности ПДн, а также за соблюдение прав и свобод субъектов ПДн в отношении их ПДн, обрабатываемых в Компании, в том числе прав на неприкосновенность частной жизни, личную и семейную тайну.

9.2. Работники Компании несут персональную ответственность за соблюдение требований по обработке и обеспечению безопасности ПДн, установленных настоящим Положением и другими локальными нормативно-правовыми актами Компании в соответствии с законодательством Российской Федерации.

9.3. Работник Компании может быть привлечен к ответственности в случаях:

- умышленного или неосторожного раскрытия ПДн;
- утраты материальных носителей ПДн;
- нарушения требований настоящего Положения и других локальных нормативных документов Компании в части вопросов доступа и работы с ПДн.

9.4. В случаях нарушения установленного порядка обработки и обеспечения безопасности ПДн, несанкционированного доступа к ПДн, раскрытия ПДн и нанесения Компании, а также субъектам ПДн, обрабатываемых в Компании, материального или иного ущерба, виновные лица несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Приложение 1

Типовое поручение на обработку персональных данных

В соответствии с Федеральным законом «О персональных данных» № 152-ФЗ от 27 июля 2006 года под персональными данными (далее – ПДн) понимается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн); под обработкой персональных данных понимается 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 (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

Исполнитель (организация, осуществляющая обработку ПДн по поручению) обязан соблюдать принципы и правила обработки ПДн, предусмотренные ФЗ-152 «О персональных данных», а также принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, возложенных на него договором, в соответствии с требованиями ФЗ-152 «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами, политикой Заказчика в отношении обработки ПДн, и принятыми Исполнителем локальными нормативными правовыми актами.

Исполнитель вправе осуществлять следующие действия с ПДн субъектов: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн *(указать нужное).*

Целями обработки ПДн Исполнителем являются:

(указать нужное в соответствии с перечнем целей обработки, утвержденным Заказчиком)

Исполнитель обязан обеспечить конфиденциальность ПДн, ставших ему известными при исполнении обязанностей по настоящему договору, а также безопасность персональных данных при их обработке в соответствии с требованиями Федерального закона «О персональных данных» № 152-ФЗ от 27.07.06 и других определяющих случаи и особенности обработки ПДн федеральных законов.

При обработке ПДн Исполнитель обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении ПДн, в том числе (выбрать нужное):

- определение угроз безопасности ПДн при их обработке в информационных системах персональных данных(далее –ИСПДн);
- применение 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;
- применение прошедших в установленном порядке процедур оценки соответствия Средств Защиты Информации;
- оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;
- учет машинных носителей ПДн;
- обнаружение фактов несанкционированного доступа к ПДн и принятие мер;
- восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установление правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечение регистрации и учета всех действий, совершаемых с ПДн в ИСПДн;
- контроль за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ИСПДн.

Привлечение Исполнителем к обработке ПДн субъектов Субисполнителей без предварительного письменного согласия Заказчика запрещено.

Субисполнители, получающие доступ к ПДн (допущенные к обработке ПДн) с согласия Заказчика, а также третьи лица, получающие доступ к ПДн на законном основании, также должны обеспечивать конфиденциальность таких данных.

Исполнитель несет ответственность перед Заказчиком за свои действия по обработке ПДн субъектов. В случае если Исполнитель привлекает (допускает) к обработке ПДн другое лицо (Субисполнителя), Исполнитель несет ответственность перед Заказчиком за действия такого лица как за свои собственные.

Трансграничная передача ПДн Исполнителем Субисполнителю и/или третьим лицам может осуществляться только при наличии предварительного согласия (письменного согласия) субъекта ПДн (в случае осуществления трансграничной передачи).

Исполнитель обязуется использовать ПДн, ставшие ему известными при исполнении обязанностей по настоящему Договору, только для выполнения работ (оказания услуг), определенных настоящим Договором.

Исполнитель обязуется обрабатывать ПДн субъектов ПДн до окончания срока действия Договора и/или до наступления одного из следующих событий, в зависимости от того, что наступит ранее:

- получение Исполнителем от Заказчика уведомления о необходимости прекращения обработки ПДн субъектов ПДн;
- достижение Исполнителем цели обработки ПДн субъектов ПДн или утраты необходимости в достижении такой цели;
- прекращение (в т.ч. при отзыве Заказчиком, исполнении, не ограничиваясь указанным) соответствующего поручения Заказчиком Исполнителю на обработку ПДн;
- прекращение действия Договора по любому основанию.

Исполнитель обязуется обеспечить блокирование, уточнение или уничтожение ПДн субъекта ПДн на основании соответствующего запроса (указания) Заказчика в сроки, установленные в таком запросе (указании), а также в иных случаях, определяемых в соответствии с законом.

Заказчик имеет право в любой момент проверить соблюдение Исполнителем требований действующего законодательства РФ о ПДн в рамках исполнения Договора. Исполнитель обязуется в той степени и таким образом, чтобы это не нарушало права субъектов ПДн, предоставить работнику Заказчика доступ к информационным системам и документам для подтверждения выполнения Исполнителем обязательств по приложению и Договору в части обработки и обеспечения безопасности ПДн в течение не более _____ рабочих дней *(указать необходимое количество дней)*.

Исполнитель должен незамедлительно в письменном виде сообщать Заказчику обо всех случаях утечки, раскрытия ПДн или их использования третьими лицами.

Приложение 2

Форма заявления о согласии работника на обработку персональных данных (передачу / получение)

ЗАЯВЛЕНИЕ

Дата _____ № _____

О согласии на обработку персональных данных

_____
должность руководителя кадровой службы организации

_____
наименование и адрес организации

_____
инициалы и фамилия руководителя

от _____
фамилия, инициалы заявителя

_____
должность работника и наименование структурного подразделения

_____
Данные документа, удостоверяющего личность и адрес регистрации

Не возражаю против _____ Вами сведений обо мне, содержащих
получения/сообщения

данные о _____
перечень персональных данных

_____
указать, откуда могут быть получены или куда переданы персональные данные

с целью _____
указать цель обработки персональных данных

Приложение 3

Форма Акта об уничтожении персональных данных

УТВЕРЖДАЮ

_____

«___» _____ 20___ г.

АКТ № _____

об уничтожении персональных данных субъекта(ов) персональных данных

Мною, _____

(должность, ф.и.о.)

в присутствии _____ _____

(должность, ф.и.о.)

_____

_____

(должность, ф.и.о.)

составлен настоящий Акт о том, что персональные данные согласно перечню:

Дата	Количество субъектов	Причина уничтожения (достижение цели обработки и/или иное)	Тип носителя информации (электронный/бумажный) и/или наименование ИСПДн	Учетный номер носителя (при наличии)	Производимая операция (стирание, уничтожение, обезличивание)
1	2	3	4	5	6

уничтожены.

Правильность произведенных записей в акте проверена.

Регистрационные данные на носителях информации (перед стиранием с них информации) с записями в акте сверены, произведено стирание содержащейся на носителях информации.

Регистрационные данные на носителях информации (твердой копии) перед их (носителей) уничтожением сверены с записями в акте и полностью уничтожены путем _____

_____.

Произведено уничтожение персональных данных в информационной системе персональных данных

_____

(наименование ИСПДн).

Отметки о стирании информации (уничтожении носителей информации) в учетных формах произведены.

_____

(Ф.И.О., подпись, дата)

_____

(Ф.И.О., подпись, дата)

Приложение 4

ЖУРНАЛ
учета обращения субъектов персональных данных

1.1 Журнал учета обращений субъектов персональных данных ведется с целью обеспечения защиты права субъекта персональных данных на получение информации об обработке его персональных данных ООО «КИВИ Блокчейн Технологии» (далее – Компания) (адрес местонахождения – г. Москва, Каширское ш., д. 70, корп. 3), предусмотренных статьей 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

1.2 Журнал ведется до его полного заполнения и хранится в Отделе кадров в течение трех лет с даты его окончания, после чего передается на архивное хранение установленным в Компании порядком.

1.3 Записи в журнале, в том числе содержащие персональные данные обратившихся в Компанию субъектов персональных данных, делаются на основании информации, содержащейся в запросе субъекта и подготовленного ответственным структурным подразделением ответа.

1.4 Запрос субъекта должен содержать:

- номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя и сведения о дате выдачи указанного документа и выдавшем его органе;
- сведения, подтверждающие участие субъекта персональных данных в отношениях с Компанией (номер договора, дата заключения договора, и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором (копию письмо или иного сообщения, полученного субъектом от Компании, проверяемые сведения о телефонном звонке работника Компании и т.п.);
- подпись субъекта персональных данных или его представителя.

1.5 Поступивший запрос после получения его Компанией передается для подготовки ответа в структурное подразделение, в ведении которого находится запрашиваемая субъектом информация.

1.6 В случае, если запрос не содержит сведений, указанных в п.1.4 настоящего документа, Компанией готовится отказ в удовлетворении полученного запроса.

1.7 После подготовки ответа в Журнале делается соответствующая отметка и излагается краткое содержание ответа, после чего ответ передается лично работником отдела кадров субъекту ПДн (при предъявлении документа, удостоверяющего его личность) или передается в Отдел документационного обеспечения для направления его субъекту почтовым отправлением с подтверждением о вручении.

1.8 Персональные данные субъектов, указанные в Журнале, обрабатываются как с использованием, так и без использования средств автоматизации, включая их сбор (получение от субъекта), запись, накопление, хранение, обновление при подготовке ответа субъекту, извлечение, использование, передачу в структурное подразделение для подготовки ответа субъекту.

1.9 Включенные в Журнал персональные данные не распространяются Компанией и не передаются в другие организации, к ним не предоставляется доступ лиц, не являющихся работниками Компании, за исключением предусмотренных законом случаев.

1.10 Типовые формы запросов, ответов на запросы и журнала учета обращений субъектов персональных данных приведены ниже.

Форма отзыва согласия на обработку персональных данных

В соответствии с ч.2 ст.9 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных»

ООО «КИВИ БЛОКЧЕЙН ТЕХНОЛОГИИ» г. Москва, Каширское ш., д. 70, корп. 3

от

_____

(фамилия, имя, отчество)

паспорт серии _____ номер _____

выданный

_____

(дата выдачи)

_____

(кем выдан)

адрес:

_____

(адрес места жительства)

ЗАЯВЛЕНИЕ

об отзыве согласия на обработку персональных данных

Я,

_____

(фамилия, имя, отчество)

(Заполняется в случае отзыва согласия представителем субъекта персональных данных)

действуя от имени

_____

(фамилия, имя, отчество)

паспорт серии _____ номер _____ выданный _____

(дата выдачи)

_____

(кем выдан)

на основании доверенности

_____

(реквизиты доверенности или иного документа, подтверждающего полномочия представителя)

в соответствии с частью 2 статьи 9 Федерального закона от 27.07.2006 г.№ 152-ФЗ «О персональных данных» отзываю согласие на обработку ООО «КИВИ БЛОКЧЕЙН ТЕХНОЛОГИИ» следующих персональных данных:

_____

(перечень персональных данных, в отношении которых отзывается согласие)

в связи с

_____

(причина отзыва согласия)

_____ _____ _____

(дата) (подпись) (расшифровка подписи)

Форма запроса субъекта на предоставление сведений об обработке персональных данных

В соответствии со ст.14 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных»

ООО «КИВИ БЛОКЧЕЙН ТЕХНОЛОГИИ» г. Москва, Каширское ш., д. 70, корп. 3

от

_____

(фамилия, имя, отчество)

паспорт серии _____ номер _____

выданный

_____

(дата выдачи)

_____

(кем выдан)

адрес:

_____

(адрес места жительства)

ЗАПРОС/ПОВТОРНЫЙ ЗАПРОС

на предоставление сведений об обработке персональных данных

Я,

_____

(фамилия, имя, отчество)

(Заполняется в случае, если запрос направляется представителем субъекта персональных данных)

действуя от имени

_____

(фамилия, имя, отчество)

паспорт серии _____ номер _____ выданный _____

(дата выдачи)

_____

(кем выдан)

на основании доверенности

_____

(реквизиты доверенности или иного документа,
подтверждающего полномочия представителя)

в соответствии со статьей 14 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» прошу предоставить следующие сведения, касающиеся обработки моих (его/её) персональных данных ООО «КИВИ БЛОКЧЕЙН ТЕХНОЛОГИИ» (нужное подчеркнуть):

подтверждение факта обработки персональных данных ООО «КИВИ БЛОКЧЕЙН ТЕХНОЛОГИИ»;

правовые основания обработки персональных данных;

цели обработки персональных данных;

способы обработки персональных данных;

сведения о лицах, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора или федерального закона;

источник получения персональных данных;

перечень обрабатываемых персональных данных;

содержание обрабатываемых персональных данных;

сроки обработки персональных данных, в том числе сроки их хранения;

порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных»;

информацию об осуществленной или о предполагаемой трансграничной передаче персональных данных;

наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению ООО «КИВИ БЛОКЧЕЙН ТЕХНОЛОГИИ», если обработка поручена или будет поручена такому лицу;

иные сведения

_____

(иные сведения, предусмотренные федеральными законами)

Запрос направляется на основании

_____

(сведения, подтверждающие участие субъекта персональных данных в отношениях с ООО «КИВИ БЛОКЧЕЙН ТЕХНОЛОГИИ» (номер договора, дата заключения договора, условное словесное обозначение и/или иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных ООО «КИВИ БЛОКЧЕЙН ТЕХНОЛОГИИ»)

Заполняется в случае, если запрос направляется повторно

Повторный запрос направляется в связи с:

_____

(указать причину повторного запроса)

_____ _____ _____

(дата) (подпись) (расшифровка подписи)

Форма ответа на запрос/повторный запрос на предоставление сведений об обработке персональных данных

В соответствии с ч.2 ст.14, ч.1 ст. 20 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных»

ООО «КИВИ БЛОКЧЕЙН ТЕХНОЛОГИИ»

г. Москва, Каширское ш., д. 70, корп. 3

Кому: _____

(фамилия, имя, отчество)

_____

(адрес места жительства)

ОТВЕТ

на запрос/повторный запрос на предоставление сведений
об обработке персональных данных №_____ от _____

Уважаемый(ая) _____

(фамилия, имя, отчество)

В соответствии с Вашим запросом от _____ уведомляем Вас

(дата запроса)

о том, что

_____

_____

_____

(запрошенные сведения об обработке персональных данных)

_____ _____ _____

(должность работника ООО «КИВИ БЛОКЧЕЙН ТЕХНОЛОГИИ») (подпись) (расшифровка подписи)

Форма отказа в предоставлении сведений/повторном предоставлении сведений об обработке персональных данных

В соответствии с ч.6, ч. 8 ст.14 и ч.2 ст.20 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных»

ООО «КИВИ БЛОКЧЕЙН ТЕХНОЛОГИИ»

г. Москва, Каширское ш., д. 70, корп. 3

Кому:

_____

(фамилия, имя, отчество)

_____

(адрес места жительства)

ОТКАЗ

в предоставлении/повторном предоставлении сведений
об обработке персональных данных №_____от_____

Уважаемый (ая)

_____

(фамилия, имя, отчество)

Вам отказано в предоставлении сведений по Вашему запросу от

_____

(дата запроса)

на основании

_____

(ссылка на ч.8 ст.14, ч.6 ст.14 Федерального закона №152-ФЗ «О персональных данных» или положения иных федеральных законов, являющихся основанием для отказа)

_____ _____ _____

(должность работника ООО «КИВИ БЛОКЧЕЙН ТЕХНОЛОГИИ») (подпись) (расшифровка подписи)

Форма уведомления об обработке персональных данных

В соответствии с положениями ч.3 ст.18 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных»

ООО «КИВИ БЛОКЧЕЙН ТЕХНОЛОГИИ»

г. Москва, Каширское ш., д. 70, корп. 3

Кому: _____

(фамилия, имя, отчество)

Адрес: _____

(адрес места жительства)

УВЕДОМЛЕНИЕ

об обработке персональных данных _____№_____

Уважаемый (ая) _____

(фамилия, имя, отчество)

Уведомляем Вас о том, что оператор персональных данных ООО «КИВИ БЛОКЧЕЙН ТЕХНОЛОГИИ», руководствуясь:

_____

(правовое основание обработки персональных данных)

осуществляет обработку Ваших персональных данных, а именно:

_____

(перечень персональных данных)

полученных _____

(источники получения персональных данных)

в целях _____

(цель обработки персональных данных)

Действия с Вашими персональными данными включают в себя

_____

(перечень действий с персональными данными)

Предполагаемыми пользователями Ваших персональных данных являются:

_____

(предполагаемые пользователи персональных данных)

Дата начала обработки персональных данных: _____

(дата)

Срок или условие прекращения обработки персональных данных:

_____

(срок или условие прекращения обработки персональных данных)

Ваши права установлены Главой 3 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».

Вы имеете право на защиту своих прав и законных интересов, в том числе обжалование действий или бездействия ООО «КИВИ БЛОКЧЕЙН ТЕХНОЛОГИИ» в отношении Ваших персональных данных, в порядке, установленном законодательством Российской Федерации.

(должность работника ООО «КИВИ БЛОКЧЕЙН ТЕХНОЛОГИИ»)	(подпись)	(расшифровка подписи)

Форма запроса на уточнение персональных данных

В соответствии с ч.1 ст.14 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных»

ООО «КИВИ БЛОКЧЕЙН ТЕХНОЛОГИИ» г. Москва, Каширское ш., д. 70, корп. 3

от

_____

(фамилия, имя, отчество)

паспорт серии _____ номер _____

выданный

_____

(дата выдачи)

_____

(кем выдан)

адрес:

_____

(адрес места жительства)

ЗАПРОС

на уточнение персональных данных

Я,

_____

(фамилия, имя, отчество)

(Заполняется в случае, если запрос направляется представителем субъекта персональных данных)

действуя от имени

_____

(фамилия, имя, отчество)

паспорт серии _____ номер _____ выданный _____

(дата выдачи)

_____

(кем выдан)

на основании доверенности

_____

(реквизиты доверенности или иного документа,
подтверждающего полномочия представителя)

в соответствии с частью 1 статьи 14 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» прошу внести изменения в мои (его/её) персональные данные

_____

(перечень изменений)

на основании сведений, содержащихся в следующих документах:

_____

(перечень документов)

_____ _____ _____

(дата) (подпись) (расшифровка подписи)

Форма уведомления о внесении изменений в персональные данные

В соответствии с ч.3 ст.20, ч.1 и 2. ст.21 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных»

ООО «КИВИ БЛОКЧЕЙН ТЕХНОЛОГИИ»

г. Москва, Каширское ш., д. 70, корп. 3

Кому: _____

(фамилия, имя, отчество)

Адрес: _____

(адрес места жительства)

УВЕДОМЛЕНИЕ

о внесении изменений в персональные данные_____№_____

Уважаемый (ая) _____

(фамилия, имя, отчество)

В соответствии с Вашим запросом от _____ уведомляем Вас

(дата запроса)

о внесении следующих изменений в обрабатываемые ООО «КИВИ БЛОКЧЕЙН ТЕХНОЛОГИИ» персональные данные:

Наименование	Исходные данные	Новые данные

на основании предоставленных Вами документов

_____

(перечень документов)

_____ _____ _____

(должность работника ООО «КИВИ БЛОКЧЕЙН ТЕХНОЛОГИИ») (подпись) (расшифровка подписи)

Форма запроса на блокирование и/или уничтожение персональных данных

В соответствии с ч.1 ст.14 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных»

ООО «КИВИ БЛОКЧЕЙН ТЕХНОЛОГИИ» г. Москва, Каширское ш., д. 70, корп. 3

от

_____

(фамилия, имя, отчество)

паспорт серии _____ номер _____

выданный

_____

(дата выдачи)

_____

(кем выдан)

адрес:

_____

(адрес места жительства)

ЗАПРОС

на блокирование/уничтожение персональных данных

Я,

_____

(фамилия, имя, отчество)

(Заполняется в случае, если запрос направляется представителем субъекта персональных данных)

действуя от имени

_____

(фамилия, имя, отчество)

паспорт серии _____ номер _____ выданный _____

(дата выдачи)

_____

(кем выдан)

на основании доверенности

_____

(реквизиты доверенности или иного документа, подтверждающего полномочия представителя)

в соответствии с частью 1 статьи 14 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» прошу произвести блокирование/уничтожение моих (его/её) персональных данных (нужное подчеркнуть)

_____

(перечень персональных данных)

в связи с

_____

(причины блокирования/уничтожения)

(дата)	(подпись)	(расшифровка подписи)

Форма уведомления о блокировании/ прекращении обработки/ уничтожении персональных данных

В соответствии с ч.1, ч.3 и ч.5 ст.21 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных»

ООО «КИВИ БЛОКЧЕЙН ТЕХНОЛОГИИ»

г. Москва, Каширское ш., д. 70, корп. 3

Кому: _____

(фамилия, имя, отчество)

Адрес: _____

(адрес места жительства)

УВЕДОМЛЕНИЕ

о блокировании / прекращении обработки /
уничтожении персональных данных _____№_____

Уважаемый (ая) _____

(фамилия, имя, отчество)

В соответствии с Вашим запросом от _____ уведомляем Вас

(дата запроса)

о том, что обработка ООО «КИВИ БЛОКЧЕЙН ТЕХНОЛОГИИ» персональных данных:

_____

(перечень персональных данных)

была заблокирована / прекращена в связи с

_____

(причина блокирования / прекращения обработки персональных данных)

а сами данные уничтожены / будут уничтожены в течение

_____

(срок уничтожения персональных данных)

_____ _____ _____

(должность работника ООО «КИВИ БЛОКЧЕЙН ТЕХНОЛОГИИ») (подпись) (расшифровка подписи)

Форма уведомления об устранении нарушений в порядке обработки персональных данных

В соответствии с ч.3 ст.21 Федерального закона от 27.02.2006 г. № 152 ФЗ «О персональных данных»

ООО «КИВИ БЛОКЧЕЙН ТЕХНОЛОГИИ»

г. Москва, Каширское ш., д. 70, корп. 3

Кому: _____

(фамилия, имя, отчество)

Адрес: _____

(адрес места жительства)

УВЕДОМЛЕНИЕ

об устранении нарушений
в порядке обработки персональных данных _____№_____

Уважаемый (ая) _____

(фамилия, имя, отчество)

В соответствии с Вашим запросом от _____ уведомляем Вас об

(дата запроса)

устранении ООО «КИВИ БЛОКЧЕЙН ТЕХНОЛОГИИ» выявленных нарушений в порядке обработки персональных данных

_____

(перечень устранённых нарушений)

Дата возобновления обработки персональных данных: _____

(дата)

_____	_____	_____
(должность работника ООО «КИВИ БЛОКЧЕЙН ТЕХНОЛОГИИ»)	(подпись)	(расшифровка подписи)

Форма журнала учета обращения субъектов персональных данных

№№ п/п	Дата обращения, входящий номер	ФИО обратившегося субъекта и его адрес	Краткое содержание запроса субъекта	Наименование подразделения, в которое запрос направлен для подготовки ответа	Дата направления ответа на запрос субъекта и краткое содержание ответа
1	2	3	4	5	6

Приложение 5

Перечень персональных данных, обрабатываемых ООО «КИВИ БЛОКЧЕЙН ТЕХНОЛОГИИ» в информационных системах персональных данных и без использования средств автоматизации

№№ п/п	Цель обработки и ее правовые основания	Категории субъектов персональных данных	Вид обработки (автоматизированная, без использования средств автоматизации, смешанная)	Наименование ИСПДн (при наличии)	Категории обрабатываемых персональных данных	Срок обработки (хранения) или условия прекращения обработки
1	Содействие в обучении и продвижении по службе, обеспечение личной безопасности работников, контроль количества и качества выполняемой работы, обеспечение сохранности имущества, расчет и выплата заработной платы, иных вознаграждений, расчет и перечисление налогов и страховых взносов. Выполнение требований нормативных правовых актов органов государственного статистического учета Трудовой кодекс РФ № 197-ФЗ от 30.12.2001 (Гл.14 «Защита персональных данных работника»). ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных» (п.п. 1 и 5 ч. ст.6). Налоговый кодекс Российской Федерации 31.07.1998 № 146-ФЗ. Федеральный закон от 06.12.2011 № 402-ФЗ «О бухгалтерском учете». Постановление Правительства РФ от 16.04.2003 № 225 «О трудовых книжках». Распоряжение Правительства РФ от 21.03.1994 № 358-р «Об обеспечении сохранности документов по личному составу». Постановление Госкомстата России от 05.01.2004 № 1 «Об утверждении	Работники Компании (в том числе бывшие), лица, являющиеся стороной договора гражданско-правового характера	Смешанная	1С ЗУП личная папка	•фамилия, имя, отчество, •пол, •год, месяц, дата рождения и место рождения; •адрес места жительства (регистрации) или места пребывания, гражданство, •ИНН, •наименование и реквизиты документа, удостоверяющего личность, •наличие визы, •номер страхового свидетельства государственного пенсионного страхования, •номер страхового полиса, •данные об образовании, •контактные данные, включая, но, не ограничиваясь: логин, номер телефона, адрес электронной почты, номер ICQ, логин Skype, •семейное положение, •сведения о составе семьи, •сведения о долговых, кредитных и финансовых обязательствах; •реквизиты банковского счета, •сведения о водительских правах и стаж вождения, •знание иностранных языков, •сведения об образовании и повышении квалификации, •сведения о воинском учёте, •профессия, •сведения о доходах и имущественном положении, •сведения о заработной плате, •сведения о принадлежности к публичным должностным лицам, •сведения о занятии должностей в муниципальных учреждениях и государственных органах, •фото- и видеоизображение (не в целях идентификации),	а) 5 лет с даты увольнения работника в отношении сведений, включаемых в бухгалтерскую отчетность; б) 4 года с даты увольнения работника в отношении сведений, включаемых в налоговую отчетность; в) 75 лет в отношении сведений, подлежащих архивному хранению (для руководителей Компании, членов руководящих исполнительных, контрольных органов Компании, работников, имеющих государственные и иные звания, премии, награды, степени и звания – постоянно); г) 30 дней (не более 6 месяцев в случае блокировки) с момента увольнения работника). д) 1 год в отношении сведений, необходимых для прохода в центр обработки данных е) 3 месяца после увольненя работника в отношении сведений, необходимых для прохода в офис Компании.

№№ п/п	Цель обработки и ее правовые основания	Категории субъектов персональных данных	Вид обработки (автоматизированная, без использования средств автоматизации, смешанная)	Наименование ИСПДн (при наличии)	Категории обрабатываемых персональных данных	Срок обработки (хранения) или условия прекращения обработки
	унифицированных форм первичной учетной документации по учету труда и его оплаты».				•фотографии вместе с указанием полного наименования фамилии, имени и отчества для размещения на корпоративном сайте, внутренних корпоративных справочниках работников организации, •сведения об общественной деятельности, •сведения о временной трудоспособности, командировании, рабочем времени и пр. •трудовой стаж, сведения о занимаемых ранее должностях, •данные о трудовом договоре работника (номер трудового договора, дата его заключения, дата начала и дата окончания договора, вид работы, срок действия договора, наличие испытательного срока, режим труда, длительность основного отпуска, длительность дополнительного отпуска, длительность дополнительного отпуска за ненормированный рабочий день, обязанности работника, дополнительные социальные льготы и гарантии, номер и число изменения к трудовому договору, характер работы, форма оплаты, категория персонала, условия труда, продолжительность рабочей недели, система оплаты), •результаты тестирования и аттестации профессиональных навыков, •сведения о профессиональной переподготовке и повышении квалификации, •сведения о наградах, •любая другая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту ПДн).	
2	Принятие решения о возможности замещения вакантных должностей кандидатами, наиболее полно соответствующими требованиям Компании. Трудовой кодекс РФ № 197-ФЗ от 30.12.2001 (Гл.14 «Защита персональных данных работника»). ФЗ от 27.07.2006 № 152-ФЗ «О	Соискатели вакантных должностей (кандидаты для приема на работу)	Смешанная	E-staff	•Ф.И.О. •номер телефона •адрес электронной почты •контактные данные •ИНН •дата и место рождения •адрес регистрации, адрес фактического проживания	До принятия решения о приеме на работу: в отношении лиц, принятых на работу, сроки хранения определяются в п.1 данного Перечня, в отношении лиц, не принятых на работу, персональные данные уничтожаются в течение 30 дней с момента принятия решения.

№№ п/п	Цель обработки и ее правовые основания	Категории субъектов персональных данных	Вид обработки (автоматизированная, без использования средств автоматизации, смешанная)	Наименование ИСПДн (при наличии)	Категории обрабатываемых персональных данных	Срок обработки (хранения) или условия прекращения обработки
	персональных данных» (п.5 ч.1 ст.6).				•предполагаемая вакансия •данные резюме •результаты тестирования профессиональных навыков •информация из предложения о работе •паспортные данные •образование •биографические данные •размер заработной платы •номер пенсионного свидетельства •наличие визы •сведения об общественной деятельности •гражданство	
3	Предоставление работникам льгот и гарантий, предусмотренных федеральным законодательствам для лиц, имеющих (усыновивших) детей, лиц с семейными обязанностями. Выполнение требований нормативных правовых актов органов государственного статистического учета Трудовой кодекс РФ № 197-ФЗ от 30.12.2001 (Глава 41 «Особенности регулирования труда женщин, лиц с семейными обязанностями»). Постановление Госкомстата России от 05.01.2004 № 1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты».	Родственники работника	Смешанная	1С ЗУП, личная папка	•ФИО •Степень родства •Год рождения •Для детей и лиц, находящихся на иждивении Работника дополнительно: •Сведения об основном документе, удостоверяющем личность (серия, номер, дата выдачи, выдавший орган) •Дата рождения •Место рождения	а) 5 лет с даты увольнения работника в отношении сведений, включаемых в бухгалтерскую отчетность; б) 4 года с даты увольнения работника в отношении сведений, включаемых в налоговую отчетность; в) 75 лет в отношении сведений, подлежащих архивному хранению (для руководителей Компании, членов руководящих исполнительных, контрольных органов Компании, работников, имеющих государственные и иные звания, премии, награды, степени и звания – постоянно); г) 30 дней (не более 6 месяцев в случае блокировки) с момента увольнения работника в отношении данных, не указанных в п.п. а, б и в).

№№ п/п	Цель обработки и ее правовые основания	Категории субъектов персональных данных	Вид обработки (автоматизированная, без использования средств автоматизации, смешанная)	Наименование ИСПДн (при наличии)	Категории обрабатываемых персональных данных	Срок обработки (хранения) или условия прекращения обработки
6	Заключение и исполнение договоров с Компанией. Гражданский кодекс РФ, Часть первая от 30.11.1994 № 51-ФЗ. Федеральный закон от 08.08.2001 № 129-ФЗ «О государственной регистрации юридических лиц и индивидуальных предпринимателей».	Представители контрагентов Компании и/или контрагенты, с которыми у Компании существуют договорные отношения или с которыми оно намерено вступить в договорные отношения	Смешанная	документы на бумажных носителях, терминальный процессинг	•ФИО •Должность •Номер телефона и иные контактные данные	До прекращения отношений с контрагентами. В отношении сведений, включенных в документы, подлежащие архивному хранению, - в соответствии с требованиями к архивному хранению.
7	Осуществление прав и законных интересов Компании или третьих лиц	Лица, по которым осуществляется курьерская доставка	Без использования средств автоматизации	документы на бумажных носителях	•ФИО •адрес доставки •Номер телефона и иные контактные данные	30 дней после достижения цели обработки
8	Исполнение обязанностей по алиментам. Федеральный закон от 02.10.2007 N 229-ФЗ «Об исполнительном производстве»	Получатели алиментов	Смешанная	1С ЗУП	•ФИО •паспортные данные •свидетельство о рождении ребенка	5 лет после достижения цели обработки
9	Правовое обеспечение и обеспечение законности деятельности Компании, а также защиты законных прав и интересов Компании ГК РФ	Лица, проходящие по судебным делам с участием Компании	Без использования средств автоматизации	документы на бумажных носителях	•ФИО •паспортные данные	5 лет после достижения цели обработки
10	Статистические или иные исследовательские цели	Участники маркетинговых исследований	Автоматизированная	Сайт SurveyMonkey	•ФИО	30 дней после достижения цели обработки

Приложение 6

Форма списка работников, допущенных к работе с ПДн в ИСПДн

№ п/п	Фамилия, имя, отчество	Подразделение	Должность	Наименование ИСПДн
1				

ПОЛОЖЕНИЕ
о порядке проведения внутренних проверок состояния защиты персональных данных в ООО «КИВИ БЛОКЧЕЙН ТЕХНОЛОГИИ»

1. Общие положения

1.1 Настоящее Положение о порядке проведения внутренних проверок состояния защиты персональных данных в ООО «КИВИ БЛОКЧЕЙН ТЕХНОЛОГИИ» (далее – Положение) регламентирует процесс проведения контроля состояния защиты персональных дынных (далее – ПДн) в ООО «КИВИ БЛОКЧЕЙН ТЕХНОЛОГИИ» (далее – Компания) и определяет перечень проверок, проводимых в рамках контроля состояния защиты ПДн.

1.2 Контроль состояния защиты ПДн проводится как для подразделений, работники которых имеют доступ и/или обрабатывают ПДн, так и для информационных систем персональных данных (далее – ИСПДн) в целях:

- обеспечения соответствия деятельности Компании требованиям законодательства Российской Федерации в части обработки и защиты ПДн;
- оценки эффективности реализованных мер обеспечения безопасности ПДн в рамках системы защиты ПДн;
- обеспечения соответствия требованиям внутренних нормативных документов Компании в области информационной безопасности (далее – ИБ).

1.3 Настоящее Положение предназначено для исполнения всеми работниками Компании, участвующими в процессе проведения проверок состояния защиты ПДн.

2 Порядок проведения контрольных мероприятий по защите персональных данных

2.1 Планирование контрольных мероприятий по защите персональных данных

2.1.1 Контрольные мероприятия по защите ПДн проводятся в соответствии с Планом проведения контрольных мероприятий по защите персональных данных (Приложение А).

2.1.2 Оценка эффективности реализованных в рамках средств защиты ПДн мер должна проводиться не реже, чем раз в 3 года.

2.1.3 Форма Плана проведения контрольных мероприятий по защите персональных данных с указанием сроков проведения плановых проверок указана в приложении (Приложение Б).

2.1.4 Контрольные мероприятия могут проводиться как Компанией самостоятельно, так и сторонней организацией. Также возможно совместное проведение проверок. В случае привлечения к проверкам сторонней организации, она (организация) должна иметь лицензию на осуществление деятельности по технической защите информации.

2.1.5 Разработанный план и сроки проведения контрольных мероприятий по защите ПДн согласовываются Менеджером по управлению отделом информационной безопасности, затем утверждаются руководством Компании. После чего утвержденный план рассылается руководителям проверяемых структурных подразделений Компании.

2.1.6 В случае необходимости проведения дополнительных (внеплановых) проверок, они инициируются Менеджером по управлению отделом информационной безопасности.

2.1.7 Для проведения контрольных мероприятий собирается Комиссия для проведения мероприятий, связанных с обработкой персональных данных (далее – Комиссия).

2.1.8 Критериями контроля обеспечения безопасности ПДн могут быть:

- требования законодательства и регуляторов в части обеспечения ИБ;
- локальные акты Компании, содержащие требования по обеспечению и управлению ИБ.

2.1.9 Выбор критериев проведения контроля осуществляется председателем Комиссии с учетом цели и области проведения контроля.

2.2 Проведение контрольных мероприятий по защите персональных данных

2.2.1 Руководители проверяемых структурных подразделений к началу проверок должны обеспечить доступность:

- необходимых для проведения проверок работников;
- необходимых для проведения проверок материалов.

2.2.2 Основными методами проведения контроля являются:

- проверка соблюдения правил обработки ПДн;
- устный опрос работников, имеющих доступ и/или обрабатывающих ПДн;
- проверка документов (структурного подразделения или проверяемых процессов);
- наблюдение за деятельностью работников;
- инструментальные проверки защищенности ИСПДн.

2.2.3 При проведении проверки должен присутствовать представитель проверяемого подразделения.

2.3 Проверки, осуществляемые в процессе проведения контрольных мероприятий по защите персональных данных

2.3.1 Контрольные мероприятия по защите ПДн подразделяются на:

- проверки организационно-правовых мероприятий;
- проверки мер обеспечения безопасности ПДн, реализованных в рамках СЗПДн;
- проверки мероприятий, направленных на недопущение воздействия на технические средства автоматизированной обработки ПДн (физическая безопасность).

2.4 Оформление результатов проведения контроля

2.3.2 Результаты контроля оформляются Комиссией в виде Акта по результатам проведения контрольных мероприятий (Приложение В). Акт подписывают председатель Комиссии и руководитель проверяемого структурного подразделения при проведении итогового совещания по результатам контроля. Все спорные вопросы и разногласия должны быть сняты до подписания Акта.

2.5 Мероприятия по результатам проведения контрольных мероприятий по защите ПДн

2.5.1 По выявленным фактам несоответствий Менеджер по управлению отделом информационной безопасности организует проведение служебного расследования, результаты которого анализируются и представляются на рассмотрение руководству Компании вместе с планом действий по всем выявленным несоответствиям.

3. Ответственность

3.1. Менеджер по управлению отделом информационной безопасности несет ответственность за:

- разработку/корректировку Плана проведения контрольных мероприятий по защите ПДн;
- реализацию контрольных мероприятий по защите ПДн;
- проведение оценки эффективности реализованных в рамках СЗПДн мер;
- взаимодействие со сторонней организацией при проведении проверок;
- разработку Отчета по результатам проведения контрольных мероприятий.

3.2. Руководители проверяемых структурных подразделений несут ответственность за участие в проведении контрольных мероприятий по защите ПДн.

3.3. Менеджер по управлению отделом информационной безопасности несет ответственность за:

- участие в согласовании Плана проведения контрольных мероприятий по защите ПДн;
- инициирование дополнительных (внеплановых) проверок (в случае необходимости);
- уведомление руководителей структурных подразделений Компании, в отношении которых проводится проверка, о проведении проверки;
- уведомление руководства Компании об итогах проведенных проверок (предоставление Отчета);
- проведение по выявленным в ходе проверки фактам несоответствий служебных расследований.

3.4. Все работники Компании несут ответственность за выполнение требований Положения, содействие и участие в проведении поверок.

4. Заключительные положения

4.1. Актуализация настоящего Положения проводится в следующих случаях:

- при изменении требований законодательства РФ в области защиты ПДн;
- по фактам возникновения инцидентов, обнаружения уязвимостей ИБ и иных значимых событий ИБ, по решению руководства Компании.

Приложение А

№ п/п	Наименование контрольного мероприятия	Вид контрольного мероприятия (периодичность и условия проведения)	Ответственное инициирующее подразделение	Краткое описание	Внутренняя отчетность
1	Проверка актуальности угроз безопасности обрабатываемых в Компании ПДн	Плановое: 1 (один) раз в год Внеплановое: при изменении технологии обработки ПДн; при изменении применимого законодательства Российской Федерации в области защиты информации	Административный отдел	Проверка актуальности угроз безопасности ПДн производится ответственными работниками Отдела информационной безопасности посредством экспертного анализа утвержденной Модели угроз безопасности персональных данных (далее – Модели угроз)	Отчетным документом, подтверждающим выполнение настоящего контрольного мероприятия, является акт, в котором отражается наличие/отсутствие необходимости пересмотра модели угроз
2	Проверка актуальности локальной нормативной базы (в том числе шаблонов, бланков, форм учета и пр.) Компании в области обеспечения безопасности ПДн с точки зрения текущих бизнес-процессов Компании и требований применимого законодательства Российской Федерации	Плановое: 1 (один) раз в год Внеплановое: при изменении технологии обработки ПДн; при изменении применимого законодательства Российской Федерации в области защиты информации	Административный отдел	Проверка актуальности локальной нормативной базы Компании в области обеспечения безопасности ПДн включает в себя проверку этих документов на предмет того, учитывают ли они все применимые требования действующего законодательства Российской Федерации в области защиты ПДн, не противоречат ли им, корректно ли описаны в них бизнес-процессы Компании (с точки зрения их соответствия практической реализации).	Отчетным документом, подтверждающим выполнение настоящего контрольного мероприятия, является акт, в котором отражается наличие/отсутствие необходимости актуализации локальных нормативных документов с указанием перечня документов
3	Проверка выполнения процедур учета, хранения и уничтожения носителей ПДн: носителей ПДн на бумажной основе и их мест хранения	Плановое: 1 (один) раз в год Внеплановое: в случае необходимости: при смене руководителей и/или работников, отвечающих за работу с носителями персональных данных на бумажной основе, при проведении служебных проверок/расследований; при смене мест хранения материальных носителей конфиденциальной информации	Административный отдел	Проверка выполнения процедур учета, хранения и уничтожения носителей ПДн на бумажной основе осуществляется ответственными работниками инициирующего подразделения в соответствии с утвержденным в Компании «Положением о порядке обработки персональных данных в ООО «КИВИ БЛОКЧЕЙН ТЕХНОЛОГИИ». При этом в случае, если в ходе проверки будет обнаружено, что утвержденные ранее места хранения не соответствуют фактическим, списки мест хранения необходимо будет обновить	Отчетным документом, подтверждающим выполнение настоящего контрольного мероприятия, является акт и обновленные списки мест хранения материальных носителей ПДн (при необходимости актуализации)

№ п/п	Наименование контрольного мероприятия	Вид контрольного мероприятия (периодичность и условия проведения)	Ответственное инициирующее подразделение	Краткое описание	Внутренняя отчетность
4	Проверка актуальности утвержденных перечней лиц:		Административный отдел		
	1) ответственных за организацию обработки ПДн	Плановое: 1 (один) раз в год		В случае необходимости актуализации, перечень редактируется и утверждается установленным в Компании порядком	Отчетными документами, подтверждающими выполнение настоящего контрольного мероприятия, являются акт и новые утвержденные перечни (при необходимости редакции перечней)
	2) ответственных за обеспечение безопасности ПДн в информационных системах	Плановое: 1 (один) раз в год			
	3) доступ которых к обрабатываемым в информационных системах персональным данным необходим для выполнения ими служебных обязанностей	Плановое: 1 (один) раз в полгода		В случае необходимости актуализации, перечень редактируется и утверждается установленным в Компании порядком.	Отчетным документом, подтверждающим выполнение настоящего контрольного мероприятия, являются акт и новые утвержденные перечни (при необходимости редакции перечней)
	4) осуществляющих обработку ПДн, либо имеющих к ним доступ (осуществляющих неавтоматизированную обработку ПДн)	Плановое: 1 (один) раз в полгода		Формирование и актуализация настоящего перечня лиц осуществляется в порядке, установленном в Положении об обработке персональных данных в ООО «КИВИ БЛОКЧЕЙН ТЕХНОЛОГИИ».	Отчетным документом, подтверждающими выполнение настоящего контрольного мероприятия, является акт и новые утвержденные перечни (при необходимости редакции перечней)
5	Проверка выполнения процедур повышения осведомленности работников по вопросам защиты персональных данных согласно требованиям действующего законодательства Российской Федерации и внутренних нормативных документов Компании (в т.ч. проверка информированности работников, осуществляющих неавтоматизированную обработку персональных	Плановое: 1 (один) раз в год	Административный отдел	Повышение осведомленности работников по вопросам защиты ПДн посредством ознакомления работников под подпись с локальными нормативными актами Компании (непосредственно перед подписанием Трудового договора). Проверка информированности работников, осуществляющих неавтоматизированную обработку ПДн, о факте и правилах осуществления такой обработки, осуществляется путем выборочной проверки отдельных Листов ознакомления работников, в процессе трудовой деятельности допущенных к материальным носителям ПДн, сверки отобранных листов с утвержденным списком лиц, допущенных до	Отчетным документом, подтверждающим выполнение настоящего контрольного мероприятия, является акт о результатах проведения проверки

№ п/п	Наименование контрольного мероприятия	Вид контрольного мероприятия (периодичность и условия проведения)	Ответственное инициирующее подразделение	Краткое описание	Внутренняя отчетность
	данных, о факте и правилах осуществления такой обработки)			неавтоматизированной обработки	
6	Проверка получения согласий работников и соискателей на обработку их персональных данных	Плановое: 1 (один) раз в год в рамках проверки выполнения процедур учета, хранения и уничтожения носителей персональных данных на бумажной основе Внеплановое: в случае необходимости: при смене руководителей и/или работников, отвечающих за работу с носителями персональных данных на бумажной основе, при проведении служебных проверок/расследований	Административный отдел	Проверка получения согласий с работников и соискателей осуществляется посредством проверки наличия в личных папках работников/соискателей подписанных письменных согласий на обработку их персональных данных	Отчетным документом, подтверждающим выполнение настоящего контрольного мероприятия, является акт о результатах проведения проверки
7	Проверка выполнения установленного процесса управления доступом к информационным активам ИСПДн	Плановое: 1 (один) раз в год Внеплановое: при проведении служебных проверок/расследований; по результатам внутреннего аудита при выявлении каких-либо несоответствий	Административный отдел	Проверка осуществляется ответственными работниками инициирующего подразделения посредством проверки перечня лиц, допущенных в систему, проверки обоснованности предоставления доступа работникам Компании в систему (наличие заявки, согласование доступа) и пр. Допускается осуществление проверки в отношении выборочного числа учетных записей	Отчетным документом, подтверждающим выполнение настоящего контрольного мероприятия, является акт с отражением информации о выявленных нарушениях
8	Проверка регистрации событий информационной безопасности	Плановое: 1 (один) раз в полгода Внеплановое: при проведении служебных проверок/расследований; по результатам внутреннего аудита при выявлении каких-либо несоответствий	Административный отдел	Осуществляется путем непосредственной проверки ведения логов информационных систем, обрабатывающих персональные данные или запроса этих логов у работников Департамента эксплуатации ИС и Департамента автоматизации финансового учета и отчетности, ответственных за системы, путем проверки регистрации событий информационной безопасности в журналах учета событий	Отчетным документом, подтверждающим выполнение настоящего контрольного мероприятия, является акт с отражением информации о выявленных нарушениях
9	Проверка регулярности обновления средств антивирусной защиты	Плановое: 1 (один) раз в полгода Внеплановое:	Административный отдел	Осуществляется путем запроса соответствующих отчетов у ответственных за средства антивирусной защиты	Отчетным документом, подтверждающим выполнение настоящего контрольного мероприятия, является акт, отражающий

№ п/п	Наименование контрольного мероприятия	Вид контрольного мероприятия (периодичность и условия проведения)	Ответственное инициирующее подразделение	Краткое описание	Внутренняя отчетность
	(актуальности вирусных баз), настроек средств антивирусной защиты	при проведении служебных проверок/расследований; по результатам внутреннего аудита при выявлении каких-либо несоответствий			результаты проверки
10	Проверка проведения резервного копирования программных средств, архивов, журналов, информационных активов, используемых и создаваемых в процессе эксплуатации ИСПДн	Плановое: 1 (один) раз в полгода Внеплановое: при проведении служебных проверок/расследований; по результатам внутреннего аудита при выявлении каких-либо несоответствий	Административный отдел	Осуществляется путем запроса соответствующих отчетов у ответственных за проведение резервного копирования работников	Отчетным документом, подтверждающим выполнение настоящего контрольного мероприятия, является акт, отражающий результаты проверки
11	Проверка проведения анализа уязвимостей информационных систем персональных данных	Плановое: 1 (один) раз в полгода Внеплановое: в случае возникновения какого-либо инцидента ИБ в соответствующей информационной системе	Административный отдел	Непосредственно анализ уязвимостей осуществляется с использованием специального программного обеспечения. Проверка проведения этого анализа осуществляется посредством запроса от работников соответствующих отчетов о выявленных за отчетный период уязвимостях и результатах/предпринятых действиях по их устранению	Отчетным документом, подтверждающим выполнение настоящего контрольного мероприятия, является акт
12	Проверка проведения оценки эффективности реализованных мер по обеспечению безопасности ПДн при их обработке в ИСПДн	Первичное: при создании системы защиты ПДн Плановое: 1 (один) раз в 3 (три) года Внеплановое: при модернизации системы защиты персональных данных	Административный отдел	Непосредственно оценка эффективности реализованных мер по обеспечению безопасности персональных данных при их обработке в ИСПДн производится в соответствии с локальными нормативными актами Компании, с учетом применения мер защиты от выявленных актуальных угроз ИБ	Отчетными документами, подтверждающими выполнение настоящего контрольного мероприятия, является акт

Приложение Б

Сроки проведения контрольных мероприятий по защите персональных данных

№	Название Подразделения (Информационной системы персональных данных)/Месяц	Январь	Февраль	Март	Апрель	Май	Июнь	Июль	Август	Сентябрь	Октябрь	Ноябрь	Декабрь
		Первое полугодие						Второе полугодие					
1.	Проверка актуальности угроз безопасности обрабатываемых в Компании ПДн												
2.	Проверка актуальности локальной нормативной базы (в том числе шаблонов, бланков, форм учета и пр.) Компании в области обеспечения безопасности персональных данных с точки зрения текущих бизнес-процессов Компании и требований применимого законодательства Российской Федерации												
3.	Проверка выполнения процедур учета, хранения и уничтожения носителей персональных данных												
4.	Проверка актуальности утвержденных перечней лиц:												
	a) ответственных за организацию обработки персональных данных												
	b) ответственных за обеспечение безопасности персональных данных в информационных системах												
	c) доступ которых к обрабатываемым в информационных системах персональным данным необходим для выполнения ими служебных обязанностей												
	d) осуществляющих обработку персональных данных либо имеющих к ним доступ (осуществляющих неавтоматизированную обработку персональных данных)												
5.	Проверка выполнения процедур повышения осведомленности работников по вопросам защиты персональных данных согласно требованиям действующего законодательства Российской Федерации и внутренних нормативных документов Компании (в т.ч. проверка информированности работников, осуществляющих неавтоматизированную обработку персональных данных, о факте и правилах осуществления такой обработки)												
6.	Проверка получения согласий работников и соискателей на обработку их персональных данных												
7.	Проверка выполнения установленного процесса управления доступом к информационным ресурсам информационных систем персональных данных												
8.	Проверка регистрации событий информационной безопасности												
9.	Проверка регулярности обновления средств антивирусной защиты (актуальности вирусных баз), настроек средств антивирусной защиты												
10.	Проверка проведения резервного копирования программных средств, архивов, журналов, информационных активов, используемых и создаваемых в процессе эксплуатации ИСПДн												
11.	Проверка проведения анализа уязвимостей ИСПДн												
12.	Проверка проведения оценки эффективности реализованных мер по обеспечению безопасности ПДн при их обработке в ИСПДн												

Приложение В

Форма акта по результатам проведения контрольных мероприятий

АКТ № _____ от «__» _____ 20__г.
о состоянии защиты персональных данных в ООО «КИВИ БЛОКЧЕЙН ТЕХНОЛОГИИ» по результатам проведения контрольных мероприятий

Группа проверки:

_____
_____
_____
_____

«____»_____201__г. проведена плановая/внеплановая проверка:

_____
_____

название подразделения (системы, процесса, участка работы)

Результат проверки:

№ п/п	Наименование контроля	Результат	Рекомендации

ПРОВЕРЯЮЩИЕ:

Должность _____/Ф.И.О.
«____»_____201__г.

Должность _____/Ф.И.О.
«____»_____201__г.

СОГЛАСОВАНО

Должность _____/Ф.И.О.
«____»_____201__г.

Должность _____/Ф.И.О.
«____»_____201__г.

Приложение 8

ПОЛОЖЕНИЕ
об обработке и защите персональных данных Работников ООО «КИВИ Блокчейн Технологии».

1. Общие положения

1.1 Настоящее Положение (далее по тексту – «Положение») разработано с целью определения порядка получения, обработки, хранения, распространения, защиты и любого другого использования персональных данных работников в соответствии с действующим законодательством Российской Федерации.

1.2 Обработка документов, содержащих персональных данных работника, может осуществляться исключительно в целях 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.

2. Обработка сведений, содержащих персональные данные работника без использования средств автоматизации

2.1. Все операции по оформлению, формированию, ведению личных папок и трудовых книжек работников должны выполняться только работниками отдела кадров, осуществляющими данную работу в соответствии со своими служебными и должностными обязанностями, зафиксированными в их должностных инструкциях.

2.2. Личные папки и трудовые книжки работников на бумажных носителях хранятся в отделе кадров. В отделе бухгалтерского учёта (бухгалтерии) могут храниться документы, содержащие персональные данные работников, которые не входят в состав личных папок работников. Все документы, содержащие персональные данные, хранятся в картотечных запирающихся шкафах, установленных в помещениях, защищенных от несанкционированного доступа. Хранение трудовых книжек работников осуществляется в соответствии с Правилами ведения и хранения трудовых книжек, изготовления бланков трудовых книжек и обеспечения ими работодателей, утвержденными Постановлением Правительства Российской Федерации. Ключи от шкафов и сейфов хранятся у уполномоченных работников отдела кадров и отдела бухгалтерского учета (бухгалтерии).

2.3. В обязанности указанных работников отдела кадров и работников отдела бухгалтерского учета (бухгалтерии), имеющих доступ к документам, содержащим персональные данные работников, входит в том числе:

- обеспечение сохранности указанных документов;
- обеспечение конфиденциальности сведений, содержащихся в документах, содержащих персональные данные работников.

3. Обработка сведений, содержащих персональные данные Работника с использованием средств автоматизации

3.1. В ООО «КИВИ БЛОКЧЕЙН ТЕХНОЛОГИИ» (далее -- Компания) внедрена система автоматического бухгалтерского расчета. Необходимые для ее функционирования сведения о работниках Компании (анкетные и биографические данные), которые в соответствии с законодательством РФ и настоящим Положением, вводятся в систему уполномоченными работниками отдела кадров.

3.2. Введенные в систему сведения о работниках подлежат защите от несанкционированного доступа наравне с документами на бумажных носителях, содержащих персональные данные Работников.

3.3. Доступ к персональным данным работников, внесенным в систему автоматического бухгалтерского учета, предоставляется:

- работникам Бухгалтерии;
- работникам Дирекции по работе с персоналом;
- работникам Департамента экономической безопасности;
- работникам Отдела информационной безопасности;
- работникам Департамента эксплуатации ИС/ Департамент автоматизации финансового учета и отчетности;
- руководству Компании.

4. Передача персональных данных Работников

4.1. Не допускается вынос личных дел работников за пределы отдела кадров, исключая Архив. Работники Компании, имеющие право доступа к документам, содержащим персональные данные работников, могут знакомиться с указанными документами только в отделе кадров. За пределы отдела кадров личные дела могут выдаваться только генеральному директору, в исключительных случаях, по письменному разрешению генерального директора, - руководителю структурного подразделения работника.

4.2. Лица, получающие документы, содержащие персональные данные работников (личные дела) во временное пользование, не имеют права делать в них пометки, исправления, вносить новые записи, извлекать документы из личной папки или помещать в нее новые.

4.3. Внутренний доступ к документам, содержащим персональные данные, для ознакомления имеют:

- генеральный директор;
- руководители структурных подразделений по направлению деятельности (доступ к личным данным только работников своего подразделения) по согласованию с руководством Компании;
- при переводе из одного структурного подразделения в другое, доступ к персональным данным работника может иметь руководитель нового подразделения;
- сам работник;
- начальник Департамента экономической безопасности и Отдела информационной безопасности;
- работники отдела кадров;
- другие работники Компании при выполнении ими своих служебных обязанностей.

4.4. Лица и органы, которым могут передаваться персональные данные без согласия работника:

- налоговые инспекции;
- правоохранительные органы;
- суды;
- органы статистики;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- подразделения муниципальных органов управления;
- государственная инспекция труда.

4.5. Указанные органы имеют доступ к персональным данным работников только в рамках своей компетенции.

4.6. Организации, в которые работник может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным работника только в случае его письменного разрешения.

4.7. Сведения о работнике или уже уволенном работнике могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии нотариально заверенного заявления работника.

4.8. Персональные данные работника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого работника.