Открытое акционерное общество
«Кольский геологический информационно-лабораторный центр» (ОАО «КГИЛЦ»)

УТВЕРЖДАЮ
Генеральный директор ОАО «КГИЛЦ»
_____ И.Н. Шахова
введено в действие приказом № 91/1
от 01 сентября 2022 г.

Для открытого пользования
Экземпляр № 01

ОАО «КГИЛЦ»
Инв. № 02-НС/ЛНА
на 20 л. лист № 1-20

П О Л И Т И К А
ОАО «КГИЛЦ» В ОТНОШЕНИИ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ ОАО «КГИЛЦ»

редакция 3

Апатиты

2022

С О Д Е Р Ж А Н И Е

Основные понятия и определения 3
1. Общие положения 5
2. Сведения об Операторе 6
3. Нормативно-правовое основание обработки персональных данных 6
4. Принципы обработки персональных данных 7
5. Цели обработки персональных данных 8
6. Категории субъектов персональных данных, категории и перечень обрабатываемых персональных данных 9
7. Способы обработки, сроки обработки и хранения персональных данных 10
8. Условия обработки персональных данных 11
9. Передача персональных данных 12
10. Организация учёта и хранения персональных данных 13
11. Организация защиты персональных данных 14
12. Порядок уничтожения персональных данных 15
13. Обязанности и права Работника 15
14. Обязанности и права Общества 17
15. Ответственность за нарушение норм, регулирующих обработку персональных данных и нарушение требований Федерального закона 20
16. Порядок актуализация и утверждения Политики 20

ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ

Для целей настоящего документа используются следующие основные понятия и определения:

Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ – кодифицированный законодательный акт (кодекс) о труде, определяющий трудовые отношения между работниками и работодателями, и устанавливает права и обязанности работника и работодателя, регулирует вопросы охраны труда, профподготовки, переподготовки и повышения квалификации, трудоустройства, социального партнерства. Закрепляются правила оплаты и нормирования труда, порядок разрешения трудовых споров.

Федеральный закон «О Персональных данных» от 27.07.2006 № 152-ФЗ – закон, регулирующий отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами, органами местного самоуправления, иными муниципальными органами, юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту Персональных данных).

Субъект персональных данных – физическое лицо, которое прямо или косвенно определено или определяется с помощью персональных данных.

Конфиденциальность персональных данных – обязательное требование для соблюдения назначенным ответственным лицом, получившим доступ к персональным данным работника, не допускать их распространения без согласия работника или иного законного основания.

Общедоступные персональных данных – персональных данных, доступ к которым предоставлен неограниченному кругу лиц с согласия работника или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

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

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

Защита персональных данных – комплекс мероприятий технического, организационного и организационно-технического характера, направленных на защиту сведений, относящихся к определённому или определяемому на основании такой информации субъекту персональных данных.

Информационная система персональных данных – совокупность программных и технических средств, на которых обрабатываются Персональных данных.

Автоматизированная обработка персональных данных – обработка конфиденциальной информации с помощью средств вычислительной техники.

Неавтоматизированная обработка персональных данных – обработка конфиденциальной информации, осуществляемая при непосредственном участии человека.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Средства защиты информации – совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных вещных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности

защищаемой информации.

Право доступа (к конфиденциальной информации) – совокупность правил доступа к защищаемой информации, установленных правовыми документами или собственником (владельцем) информации.

Несанкционированный доступ – доступ к информации, осуществляемый с нарушением установленных прав и (или) правил доступа к информации.

Распространение персональных данных – санкционированные действия, направленные на передачу Персональных данных определенному кругу лиц или на ознакомление с Персональными данными.

Предоставление персональных данных – санкционированные действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

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

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

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

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

Разглашение информации – несанкционированное доведение защищаемой информации до лиц, не имеющих права доступа к этой информации.

Безопасность информации – состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.

Угроза безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных.

Уровень защищенности персональных данных – комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Носитель информации – материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Автоматизированное рабочее место – рабочее место специалиста, оснащенное персональным компьютером, программным обеспечением и совокупностью информационных ресурсов индивидуального или коллективного пользования, которые позволяют ему вести обработку данных.

Уполномоченный орган по защите прав субъектов персональных данных – федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных.

Федеральная служба по аккредитации (Росаккредитация) – федеральный орган исполнительной власти, осуществляющий функции по формированию единой национальной системы аккредитации и осуществляющий контроль за деятельностью аккредитованных лиц, а также уполномоченный федеральный орган исполнительной власти, осуществляющий функции национального органа Российской Федерации по аккредитации.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий документ разработан в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О Персональных данных» (далее – Федеральный закон), а также с Трудовым кодексом Российской Федерации от 30.12.2001 № 197-ФЗ (далее – ТК РФ) и является основополагающим внутренним регулятивным документом ОАО «КГИЛЦ» (далее – Общество).

1.2. Цель разработки настоящей политики в отношении обработки и защиты персональных данных работников в Обществе (далее – Политика) – обеспечение защиты прав и свобод человека и гражданина, при обработке его персональных данных, в том числе права на неприкосновенность частной жизни, личную и семейную тайну, защиту чести и достоинства личности, гарантированных ей Конституцией Российской Федерации.

1.3. Политика определяет позицию и намерения Общества его деятельности в области обработки персональных данных субъектов персональных данных (далее – Работники) и реализуемых мер по их защите. Сведения о персональных данных Работников (далее – Персональные данные) Общества относятся к категории конфиденциальной информации, составляющей охраняемую законом тайну Общества.

1.4. В Политике используются термины и определения в соответствии с их назначениями, как они определены в Федеральном законе и принятыми в соответствии с ним нормативными правовыми актами.

1.5. Настоящая Политика определяет и регламентирует:

- закрепление нормативной и организационно-правовой базы в отношении сведений, составляющих Персональные данные;
- состав целей и способов обработки Персональных данных;
- основные условия, порядок и способы обработки Персональных данных;
- категории, объём и перечень Персональных данных;
- категории субъектов, Персональные данные которых обрабатываются;
- сроки обработки и хранения Персональных данных;
- организацию учёта и хранения Персональные данных;
- порядок уничтожения Персональных данных при достижении целей их обработки или при наступлении иных законных оснований;
- обязанности и права Работников, Персональные данные которых подлежат обработке;
- обязанности и права Общества в отношении обработки и защиты Персональных данных;
- порядок внутреннего обмена Персональными данными и их передачи третьим лицам (сторонним лицам, организациям и ведомствам);
- внутренний и внешний доступ к Персональным данным;
- порядок обработки обращений и запросов Работников или их законных представителей;
- порядок действий в случае запросов уполномоченного органа по защите прав субъектов Персональных данных;
- действия Общества для обеспечения необходимого объёма мер в области защиты Персональных данных от несанкционированного доступа, разглашения (утечки) или утраты Персональных данных;
- перечень предлагаемых законодателем мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, которые обязано принимать Общество;
- обязанности Общества по устранению нарушений законодательства, допущенных при обработке Персональных данных, по уточнению, блокированию и уничтожению Персональных данных;
- ответственность лиц, имеющих доступ к Персональным данным, осуществляющих их обработку и защиту за нарушение норм, регулирующих обработку и защиту конфиденциальной информации.

1.6. Настоящая Политика утверждается и вводится в действие приказом Генерального директора Общества (далее – Руководитель) и регламентирует действия всех сотрудников Общества, допущенных и участвующих в организации процессов обработки и обеспечения безопасности Персональных данных.

1.7. Настоящее Политика подлежит актуализации в случаях:

- внесения изменений в законодательство РФ в области обработки и защиты Персональных данных;
- внесения изменений в организационную структуру системы обеспечения информационной безопасности Общества;
- внесения изменений в локальные нормативные акты Общества, регламентирующих организацию обработки и обеспечение безопасности Персональных данных.
- изменения целей обработки Персональных данных;
- внесения изменений в организацию и порядок обработки Персональных данных;
- необходимости в изменении процесса обработки Персональных данных, связанной с деятельностью Общества;
- применения новых технологий обработки Персональных данных;
- результатов контроля выполнения требований по обработке и защите Персональных данных;

1.8. Политика обязательна для ознакомления под подпись Работниками всех структурных подразделений, отделов и служб Общества, предоставляющих свои Персональные данные Обществу.

1.9. Настоящая Политика вступает в силу с момента утверждения её Руководителем Общества и действует до замены в очередной редакции.

1.10. Все изменения в Политике вносятся приказом Руководителя в установленном порядке.

1.11. Настоящая Политика содержит сведения, подлежащие раскрытию, является общедоступным документом Общества и предусматривает возможность ознакомления с ней любых лиц.

1.12. Актуальная версия Политики опубликована на сайте Общества https://www.kgilc.ru.

2. СВЕДЕНИЯ ОБ ОПЕРАТОРЕ

2.1. Общество как работодатель и юридическое лицо, самостоятельно осуществляющее обработку Персональных данных, связанную с трудовыми функциями Работников, является оператором Персональных данных (далее – Оператор).

2.2. Оператор – ОАО «Кольский геологический информационно-лабораторный центр» (ОАО «КГИЛЦ»).

2.3. Оператор расположен и осуществляет свою деятельность по адресу: 184209, Мурманская область, г. Апатиты, ул. Ферсмана 26В.

2.4. Генеральный директор – Шахова Инна Николаевна, действующий на основании Устава ОАО «КГИЛЦ».

2.5. ИНН Оператора – 5101600300.

2.6. ОГРН Оператора – 1025100507046.

2.7. Контактные данные: телефон/факс: (815-55) 7-66-06;

2.8. E-mail: mail@kgilc.ru.

2.9. Официальный сайт: https://kgilc.ru

3. НОРМАТИВНО-ПРАВОВОЕ ОСНОВАНИЕ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Нормативно-правовым основанием для обработки Персональных данных являются совокупность правовых актов, во исполнение которых и в соответствии с которыми Общество осуществляет обработку Персональных данных.

3.2. Правовыми актами для обработки Персональных данных Обществом являются:

- Конституция Российской Федерации (ст. 24);
- Трудовой кодекс Российской Федерации;
- Федеральный закон от 27 июля 2006 года № 152-ФЗ «О Персональных данных»;
- Федеральный закон от 14 июля 2022 г. № 266-ФЗ «О внесении изменений в Федеральный закон «О Персональных данных», отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона «О банках и банковской деятельности»;
- Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ;

- Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки Персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите Персональных данных при их обработке в информационных системах Персональных данных»;
- приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности Персональных данных при их обработке в информационных системах Персональных данных»;
- приказ Роскомнадзора от 05 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию Персональных данных»;
- приказ Гостехкомиссии России от 30.08.02 № 282 «Специальные требования и рекомендации по технической защите конфиденциальной информации»;
- указ Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»;
- приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности Персональных данных при их обработке в информационных системах Персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите Персональных данных для каждого из уровней защищенности».
- приказ Росархива от 20.12.2019 № 236 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения»;
- Кодекс Российской Федерации об административных правонарушениях;
- Гражданский кодекс Российской Федерации;
- Уголовный кодекс Российской Федерации;
- иные Федеральные законы и подзаконные акты, определяющие случаи и особенности обработки Персональных данных;
- настоящая Политика.

4. ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. При обработке Персональные данных Общество руководствуется требованиями действующего законодательства Российской Федерации в области обработки и защиты Персональных данных, а также следующими принципами:

- обработка Персональных данных осуществляется на законной и справедливой основе для выполнения возложенных законодательством функций, полномочий и обязанностей, осуществления прав и законных интересов Работников;
- обработка Персональных данных ведется с учетом обеспечения защиты прав и свобод Работников при обработке их Персональных данных, в том числе прав на неприкосновенность частной жизни, личную и семейную тайну;
- обработка Персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка Персональных данных, несовместимая с целями сбора Персональных данных;
- не допускается объединение баз данных, содержащих Персональных данных, обработка которых осуществляется в целях, несовместимых между собой.
- обработке подлежат только те Персональных данных, которые отвечают заявленным целям обработки;
- содержание и объем обрабатываемых Персональных данных соответствуют заявленным целям обработки. Обрабатываемые Персональных данных не являются избыточными по отношению к заявленным целям обработки или несовместимыми по отношению к выполнению договорных обязательств;
- при обработке Персональных данных обеспечиваются их точность, достаточность, а в необходимых случаях и актуальность по отношению к целям обработки Персональных данных;
- Общество принимает необходимые меры либо обеспечивает их принятие по удалению или уточнению неполных или неточных данных;

- хранение Персональных данных должно осуществляться в форме, позволяющей определить Работника, не дольше, чем этого требуют цели обработки Персональных данных, если срок хранения Персональных данных не установлен Федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных.
- обрабатываемые Персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено Федеральным законом.
- соблюдение принципов и правил обработки Персональных данных при поручении такой обработки другому (третьему) лицу;
- соблюдение конфиденциальности в отношении Персональных данных;
- соблюдение обязанностей, возлагаемых на Общество, действующим законодательством и иными нормативными актами Российской Федерации в области Персональных данных;
- принятие мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных законодательством в области Персональных данных;
- недопустимости ограничения прав и свобод человека и гражданина по мотивам, связанным с использованием различных способов обработки Персональных данных;
- недопустимости использования оскорбляющих чувства граждан или унижающих человеческое достоинство способов категорирования Персональных данных;
- личной ответственности должностных лиц, осуществляющих обработку Персональных данных;
- документального оформления всех принятых решений по обработке Персональных данных.

4.2. Деятельность по организации администрирования, обработки и защиты Персональных данных в соответствии с требованиями законодательства Российской Федерации о Персональных данных осуществляется уполномоченными лицами, назначенными приказом Руководителя Общества в установленном порядке.

4.3. Уполномоченные лица осуществляют обработку Персональных данных в объемах и целях, предусмотренных законодательством РФ и локальными нормативными актами Общества, а также обеспечивают их защиту от неправомерного использования, утраты, уничтожения и несанкционированного доступа к ним.

5. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Цели обработки Персональных данных происходят из анализа правовых актов, регламентирующих деятельность Общества, целей фактически осуществляемой Обществом деятельности, а также деятельности, которая предусмотрена учредительными документами Общества.

5.2. Обработка Персональных данных осуществляется Обществом исключительно в целях оформления, заключения и регулирования трудовых отношений Работников с Обществом и иных непосредственно связанных с ними отношений, а конкретно для:

- обеспечения соблюдения требований законодательства РФ;
- содействия в трудоустройстве и получения образования и продвижения по службе;
- обеспечения кадровой и бухгалтерской работы (отражения информации в кадровых и финансовых документах);
- оформления банковской карты, начисления и перечисления заработной платы в Банк ВТБ (ПАО), ПАО «Сбербанк России», АО «Почта Банк»;
- исчисления и уплаты налоговых платежей, сборов и взносов на обязательное социальное и пенсионное страхование, предусмотренных законодательством РФ;
- представления Обществом установленной законодательством отчетности в отношении физических лиц, в том числе сведений Персонифицированного учета в Пенсионный фонд РФ, сведений подоходного налога в ИФНС России, сведений в ФСС РФ;
- оформления допуска к сведениям, составляющих государственную тайну;
- заключения производственных договоров (контрактов, соглашений);
- заключения возмездных договоров (подряда, оказания услуг, аренды);
- оформления договоров гражданско-правового характера;
- оформления заявок для участия в конкурсах и тендерах;

- аккредитации структурных подразделений в Федеральной службе по аккредитации и предоставления сведений о результатах своей деятельности;
- составления штатного расписания;
- обучения (повышения квалификации) Работников;
- прохождения Работниками медицинских профосмотров;
- оформления пропусков в ЗАТО;
- оформления командировок;
- отправки корреспонденции;
- обеспечения безопасности Работников и сохранности имущества Общества;
- контроля количества и качества выполняемой работы Работниками.

6. КАТЕГОРИИ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ, КАТЕГОРИИ И ПЕРЕЧЕНЬ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. К категориям субъектов персональных данных. относятся физические лица – граждане Российской Федерации, а также иностранные граждане, предоставившие свои Персональных данных и давших согласие на их обработку Обществу.

6.2. Обществом обрабатываются общие и биометрические категории Персональных данных физических лиц, к которым относятся Работники Общества, члены их семей, уволенные Работники.

6.3. Общество обрабатывает следующий перечень Персональных данных, к которым относятся:

- биометрические данные (фотография) – предоставление не обязательно, в соответствии ч. 3 ст. 11 Федерального закона;
- фамилия, имя, отчество (в том числе предыдущие фамилии, имена и отчества, в случае их изменения);
- число, месяц, год рождения;
- место рождения;
- сведения о гражданстве (в том числе предыдущие и иные гражданства);
- сведения, указанные в анкете, предоставляемой при поступлении на работу;
- сведения, указанные в резюме (автобиографии);
- паспортные данные (серия, номер документа, дата выдачи, наименование органа его выдавшего);
- адрес и дата регистрации по месту жительства (месту пребывания);
- адрес фактического проживания;
- контактная информация (номер домашнего/мобильного телефона, e-mail) или сведения о других способах связи;
- идентификационный номер налогоплательщика (ИНН);
- реквизиты страхового свидетельства обязательного пенсионного страхования (СНИЛС);
- реквизиты полиса обязательного медицинского страхования (полиса ОМС);
- реквизиты свидетельства государственной регистрации актов гражданского состояния (семейное Политика);
- сведения, содержащиеся в свидетельстве о рождении ребёнка (детей);
- заключение медицинского учреждения о наличии (отсутствии) заболевания, препятствующего поступлению на работу и её осуществление;
- реквизиты документов воинского учёта и сведения, содержащиеся в документах воинского учёта (для военнообязанных и лиц, подлежащих призыву на военную службу);
- сведения об образовании (когда и какие образовательные учреждения закончил(а), реквизиты дипломов, направление подготовки, специальность и квалификация по диплому);
- сведения о послевузовском профессиональном образовании (наименование образовательного или научного учреждения, год окончания), ученой степени, ученом звании (когда присвоены, номера дипломов, аттестатов);
- сведения о профессиональной переподготовке и (или) повышении квалификации (реквизиты документов о профессиональной переподготовке и (или) повышении квалификации);
- сведения о государственных наградах РФ, иных наградах и знаках отличия (кем награжден(а) и когда);
- сведения о реквизитах трудовой книжки (вкладыша в неё);

- сведения, содержащиеся в трудовой книжке;
- сведения о трудовой деятельности (данные о трудовой занятости на текущее время);
- сведения с предыдущего места работы (справки 2-НДФЛ, о начисленных и уплаченных страховых взносах);
- содержание и реквизиты трудового договора и дополнительных соглашений к нему;
- сведения о кадровых приказах (приеме на работу, перемещении по должности, увольнении);
- сведения о заработной плате;
- сведения о поощрениях (премиях, вознаграждениях), наказаниях;
- сведения о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения заработной платы;
- сведения о командировках;
- сведения, содержащиеся в листке временной нетрудоспособности работника;
- сведения об обязательствах по материальному обеспечению (алиментах);
- номера Персональных счетов в кредитно-финансовых организациях или банковских карт (для перечисления причитающихся финансовых средств);
- сведения о допуске к государственной тайне, оформленному за период работы, службы, учебы (форма, номер и дата);
- данные заграничного паспорта (серия, номер, кем и когда выдан);
- сведения о владении иностранными языками и языками народов РФ;
- сведения о степени родства с близкими родственниками;
- фамилии, имена, отчества близких родственников (отца, матери, братьев, сестер, детей), а также мужа (жены);
- даты рождения, места рождения и адреса проживания близких родственников;
- сведения о местах работы, должностях близких родственников;
- прежние фамилии мужей (жён) (в случае изменения);
- фамилии, имена, отчества, даты рождения, места рождения, места работы и домашние адреса бывших мужей (жен);
- сведения о пребывании за границей (когда, где, с какой целью);
- сведения о близких родственниках (отца, матери, братьях, сестрах, детях), а также муже (жене), в том числе бывших, постоянно проживающих за границей и (или) оформляющие документы для выезда на постоянное место жительства в другое государство (фамилии, имена, отчества, с какого времени проживают за границей);
- наличие (отсутствие) судимости;
- наличие (отсутствие) судимости у близких родственников;
- материалы служебных расследований (акты, докладные записки, протоколы, протоколы комиссии по трудовым спорам и др.);
- аудиозаписи и видеозаписи с участием Работника.

6.4. Предоставление Работником биометрических персональных данных не может быть обязательным, за исключением случаев, предусмотренных Федеральным законом.

7. СПОСОБЫ ОБРАБОТКИ, СРОКИ ОБРАБОТКИ И ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Обработка Персональных данных осуществляется Обществом путём смешанной обработки Персональных данных – как с использованием средств автоматизации, так и без использования таких средств, с передачей полученной информации по защищенным информационно-телекоммуникационным сетям Интернет.

7.2. Перечень действий по обработке Персональных данных (без ограничений) включает следующее:

- сбор, запись, систематизацию, накопление, хранение;
- уточнение (обновление, изменение);
- передачу (предоставление, доступ);
- извлечение, использование;
- обезличивание, блокирование, удаление и уничтожение;
- осуществление иных действий с предоставленными Персональными данными, предусмотренных действующим законодательством РФ.

7.3. Сроки обработки Персональных данных должны ограничиваться достижением конкретных, заранее определённых и законных целей.

7.4. Срок обработки Персональных данных Обществом исчисляется с момента подписания Работником согласия на обработку его Персональных данных (далее – Согласие) и действует до наступления одного из перечисленных событий:

- расторжения трудового договора (увольнения);
- отзыва Согласия в письменной форме или в форме электронного документа, подписанного в соответствии с Федеральным законом электронной подписью в соответствии с действующим законодательством РФ;
- истечения сроков, установленных действующим законодательством РФ, после чего Персональные данные подлежат хранению и уничтожению в течение сроков, установленных законодательством РФ.

7.5. Хранение Персональных данных должно осуществляться в форме, позволяющей определить Работника, не дольше, чем этого требуют цели обработки Персональных данных, если срок хранения Персональных данных не установлен Федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является Работник.

7.6. После увольнения Работника Общество продолжает хранить его Персональные данные для начисления, удержания и перечисления налогов за последний месяц работы, отчётности в фонды и налоговую инспекцию, предоставления документов проверяющим структурам.

8. УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Обработка Персональных данных осуществляться Обществом с соблюдением принципов и правил, предусмотренных Федеральным законом.

8.2. В случаях, предусмотренных Федеральным законом, обработка Персональных данных осуществляется только с Согласия в письменной форме Работника или его законного представителя.

Равнозначным содержащему собственноручную подпись Работника или его законного представителя Согласию в письменной форме на бумажном носителе признается Согласие в форме электронного документа, подписанного в соответствии с Федеральным законом электронной подписью.

8.3. Работник принимает решение о предоставлении его Персональных данных и дает Согласие на их обработку свободно, своей волей и в своем интересе, подтверждая достоверность указанных сведений.

Согласие должно быть конкретным, предметным, информативным, сознательным и однозначным.

8.4. Согласие в письменной форме должно включать в себя, в частности:

- фамилию, имя, отчество, адрес Работника, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- фамилию, имя, отчество, адрес законного представителя Работника, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого законного представителя (при получении Согласия от законного представителя Работника);
- наименование или фамилию, имя, отчество и адрес Оператора, получающего Согласие;
- цель обработки Персональных данных;
- перечень Персональных данных, на обработку которых дается Согласие;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку Персональных данных по поручению Общества, если обработка будет поручена такому лицу;
- перечень действий с Персональными данными, на совершение которых дается Согласие;
- общее описание используемых Обществом способов обработки Персональных данных;
- срок, в течение которого действует Согласие, а также способ его отзыва, если иное не установлено Федеральным законом;
- подпись Работника.

8.6. В случае получения Согласия от законного представителя Работника полномочия данного законного представителя на дачу Согласия от имени Работника проверяются Обществом.

8.7. Персональные данные могут быть получены Обществом от лиц, не являющимися Работниками (от третьих лиц), при условии предоставления Обществу подтверждения наличия оснований, указанных в Федеральном законе.

8.8. Общество вправе с Согласия поручить обработку Персональных данных третьему лицу при условии соблюдения этим лицом конфиденциальности Персональных данных и обеспечения их безопасности при обработке. Лицо, которому Общество поручает обработку Персональных данных, не обязано получать Согласие от Работника на такую обработку. Ответственность перед Работником за действия третьего лица, которому Общество поручило обработку его Персональных данных, несет Общество.

8.9. Согласие может быть отозвано Работником. В случае отзыва Работником Согласия Общество вправе продолжить обработку Персональных данных без Согласия Работника при наличии оснований, указанных в Федеральном законе.

8.11. Доступ к Персональным данным имеют только сотрудники (пользователи) Общества, которым эти данные необходимы для исполнения трудовых обязанностей.

8.13. При обработке Персональных данных Общество принимает необходимые правовые, организационные и технические меры 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 Персональных данных.

8.14. Общество гарантирует, что не осуществляет принятие решений, порождающих юридические последствия в отношении Работника или иным образом затрагивающих его права и законные интересы, на основании исключительно автоматизированной обработки Персональных данных.

8.15. Общество обязано 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.

8.16. Вышеуказанная информация (за исключением информации, составляющей государственную тайну) передается федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, в уполномоченный орган по защите прав субъектов персональных данных.

8.17. Порядок передачи информации устанавливается совместно федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и уполномоченным органом по защите прав субъектов персональных данных.

8.18. Все меры конфиденциальности при обработке Персональных данных распространяются как на бумажные, так и на электронные носители конфиденциальной информации.

8.19. Процедура оформления доступа к Персональным данным предусматривает ознакомление с настоящим Политикам лиц, допущенных и участвующих в организации процессов обработки и обеспечения безопасности Персональных данных под подпись, а также истребование с них, письменного обязательства о соблюдении конфиденциальности в отношении Персональных данных.

9. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. В соответствии со ст. 88 ТК РФ при передаче Персональных данных Общество должно соблюдать следующие требования:

- не сообщать Персональные данные Работника третьей стороне без его Согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью Работника, а также в других случаях, предусмотренных ТК РФ или иными федеральными законами;
- не сообщать Персональные данные Работника в коммерческих целях без его Согласия;

- предупредить лиц, получающих Персональные данные, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие Персональные данные, обязаны соблюдать режим секретности (конфиденциальности). Данное Политика не распространяется на обмен Персональными данными в порядке, установленном ТК РФ и иными федеральными законами;
- разрешать доступ к Персональным данным только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те Персональные данные, которые необходимы для выполнения конкретных функций;
- не запрашивать и не передавать информацию о состоянии здоровья Работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения Работником своей трудовой функции;
- передавать Персональные данные его законным представителям в порядке, установленном ТК РФ и Федеральным законом, и ограничивать эту информацию только теми Персональными данными, которые необходимы для выполнения указанными представителями их функций;

9.2. Требования при передаче Персональных данных третьим лицам:

- передача Персональных данных третьим лицам осуществляется только с Согласия Работника в письменной форме;
- не допускается отвечать на вопросы, связанные с передачей Персональных данных, по телефону или факсу;
- передача Персональных данных по каналам связи, в том числе информационно-телекоммуникационным каналам посредством сети «Интернет» допускается только при использовании средств криптографической защиты;
- Персональные данные могут быть предоставлены родственникам или членам семьи Работника только с письменного разрешения самого Работника, за исключением случаев, когда передача Персональных данных без его Согласия допускается действующим законодательством РФ.
- сведения о Персональных данных или о Персональных данных уже уволенного Работника могут быть предоставлены третей стороне (организации, ведомству) только с письменного запроса на официальном бланке организации (ведомства) в случаях предусмотренных частью 1 ст. 6 Федерального закона, только в сфере своей компетенции и только в целях, для достижения которых эти Персональных данных необходимы.

10. ОРГАНИЗАЦИЯ УЧЁТА И ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1. Хранение Персональных данных осуществляется в порядке, исключающем их утрату, порчу или их неправомерное использование.

10.2. Перечень мест хранения материальных носителей с Персональными данными определяется приказом Руководителя. Хранение их осуществляется в запираемых металлических шкафах, сейфах и архивном помещении Общества.

10.3. Документы, предъявленные Работниками при приёме на работу, содержащие Персональные данные, подлежат процессу сканирования. Созданные электронные копии документов в автоматизированном режиме, переносятся в ИСПДн «Кадры ОАО «КГИЛЦ», расположенной в защищённом периметре локальной сети Общества.

10.4. Доступ ИСПДн «Кадры ОАО «КГИЛЦ» имеет ограниченный круг должностных лиц, уполномоченный приказом Руководителя, и осуществляется посредством Персональных средств аутентификации (программного комплекса VipNet Client).

10.5. Документы, содержащие Персональные данные, в электронном виде хранятся в ИСПДн «Бухгалтерия 1С» в закрытом контуре и предназначены для бухгалтерского и налогового учета, формирования необходимой отчётности.

10.6. Документы, отражающие персональную информацию об уволенных Работниках, на бумажных носителях упорядочиваются по годам и направляются в архивное помещение для хранения в соответствии со сроками, установленными Приказом Минкультуры от 25.08. 2010 № 558 и приказа Росархива от 20.12.2019 № 236 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения».

11. ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

11.1 Защита Персональных данных от неправомерного их использования или утраты обеспечивается Обществом за счёт собственных средств, в порядке, установленном ТК РФ и Федеральным законом.

11.2. Защите подлежат Персональные данные и документы, содержащие Персональные данные на материальных носителях и электронных носителях, а также Персональные данные и документы их содержащие, обрабатываемые в ИСПДн.

11.3. Для защиты Персональных данных принимаются необходимые организационные и технические меры по обеспечению их конфиденциальности, целостности и доступности к ним.

11.4. Обеспечение внутренней защиты Персональных данных.

11.4.1. Для обеспечения внутренней защиты Персональных данных Обществом применяются следующие меры:

- ограничение и регламентация состава лиц, исполнение должностных обязанностей которых требует обработки Персональных данных;
- строгое избирательное и обоснованное распределение документов и информации между лицами, имеющими доступ к Персональных данных;
- разграничение прав доступа к Персональных данных с использованием учетной записи и системой паролей от несанкционированного доступа, искажения и уничтожения, а также от иных неправомерных действий с данной информацией;
- знание лицами, имеющими доступ к Персональных данных, положений законодательства Российской Федерации в области Персональных данных и требований локальных нормативных актов Общества по защите Персональных данных и сохранению их конфиденциальности;
- рациональное размещение автоматизированных рабочих мест, на которых ведётся обработка Персональных данных, при котором исключается бесконтрольное использование защищаемой информации;
- наличие необходимых условий в помещениях для работы с конфиденциальными документами и ИСПДн;
- определение и регламентация состава лиц, имеющих право доступа (входа) в помещения, в которых обрабатываются и хранятся Персональных данных;
- определение и регламентация состава лиц, имеющих право доступа (входа) в архивное помещение;
- организация порядка уничтожения информации с Персональными данными;
- использование технических средств защиты информации;
- использование технических средств криптографической защиты информации;
- соблюдение условий хранения документов, материальных и электронных носителей с Персональными данными;
- своевременное выявление нарушений требований по защите Персональных данных, установленных в Обществе и принятие мер по устранению таких нарушений;
- профилактическая, воспитательная и разъяснительная работа по предупреждению утраты сведений при работе с конфиденциальными документами;

11.5. Для обеспечения внешней защиты Персональных данных применяются следующие меры:

- использование технических средств охраны, сигнализации;
- организация охраны территории и помещений;
- ограничение доступа посторонних лиц в помещения Общества.

11.6. Деятельность по обеспечению безопасности Персональных данных в Обществе реализовывается постоянно. В целях обеспечения эффективности мероприятий по обеспечению безопасности Персональных данных в Обществе осуществляются:

- организация эксплуатации ИСПДн в соответствии с требованиями безопасности;
- контроль выполнения и эффективности мероприятий по обеспечению безопасности Персональных данных в Обществе;
- принятие мер по устранению выявленных нарушений требований по безопасности Персональных данных;
- планирование, разработка и реализация мер по совершенствованию мероприятий по обеспечению безопасности Персональных данных.

11.7. Технические меры защиты Персональных данных при их обработке техническими средствами устанавливаются в соответствии со Специальными требованиями и

рекомендациями по технической защите конфиденциальной информации (СТР-К), утвержденными приказом Гостехкомиссии России от 30.08.2002 № 282.

11.8. Организацию мероприятий по контролю и защите Персональных данных в структурных подразделениях отделах и службах Общества осуществляют должностные лица, назначенные приказом Руководителя.

11.9. Общий контроль за соблюдением мер по защите Персональных данных осуществляет ответственное должностное лицо за организацию обработки, защиты и хранения Персональных данных, назначенное приказом Руководителя.

12. ПОРЯДОК УНИЧТОЖЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

12.1. Уничтожению подлежат утратившие практическое значение и не имеющие ценности носители информации, содержащие Персональные данные, если иное не предусмотрено Федеральным законом.

12.2. В случаях достижения цели обработки Персональных данных или отзыва Согласия Работником на обработку его Персональных данных Общество обязано незамедлительно прекратить обработку Персональных данных и уничтожить их в сроки, предусмотренные в п.4, п.5, п.6 ст. 21 Федерального закона, если иное не предусмотрено положениями данной статьи.

12.3. При уничтожении носителей с Персональных данных исключается ознакомление с ними посторонних лиц, неполное или случайное их уничтожение.

12.4. Уничтожение конфиденциальной информации с материальных носителей.

12.4.1. Для уничтожения бумажных носителей используются два вида их утилизации:

- шредирование (измельчение);
- подконтрольное сжигание.

12.4.2. Уничтожение машинных носителей заключается в таком воздействии на рабочие слои дисков и микросхемы памяти, в результате, которого разрушается физическая, магнитная или химическая структура рабочего слоя.

12.5. Уничтожение конфиденциальной информации в ИСПДн.

12.5.1. Уничтожение конфиденциальной информации, содержащей Персональные данные, в ИСПДн обеспечивается согласно инструкции по уничтожению Персональных данных в Обществе, при этом исключается возможность полного или частичного восстановления таких данных.

12.5.2. Способ уничтожения информации в ИСПДн, в которых обрабатываются Персональных данных Работников, реализуется с помощью штатных средств путём:

- удаления записей содержащих ПНд из баз данных;
- удаления логов, реплик и резервных копий баз данных;

12.6. Уничтожение Персональных данных, не подлежащих архивному хранению, осуществляется постоянно действующей комиссией по уничтожению Персональных данных (далее – Комиссия), утверждённой приказом Руководителя.

12.7. На материалы, отобранные Комиссией, составляется акт, об уничтожении материальных носителей или электронных документов с Персональными данными, который подписывается членами Комиссии и утверждаются её председателем.

12.8. Без оформления акта уничтожаются: испорченные бумажные и технические носители, черновики, проекты документов и другие материалы, образовавшиеся при исполнении документов, содержащих Персональных данных.

12.9. Уничтожение материалов, содержащих Персональные данные до утверждения акта об уничтожении документов председателем Комиссии, запрещается.

12.10. Хранение актов об уничтожении Персональных данных осуществляется в течение сроков, установленных нормативными правовыми актами РФ.

13. ОБЯЗАННОСТИ И ПРАВА РАБОТНИКА

13.1. В соответствии с положениями ст. 89 ТК РФ Работник имеет право на:

- полную информацию об его Персональных данных и обработке этих данных;
- свободный бесплатный доступ к своим Персональным данным, включая право на получение копий любой записи, содержащей Персональные данные, за исключением случаев, предусмотренных Федеральным законом;
- определение своих представителей для защиты своих Персональных данных, а также на самостоятельную защиту своих прав;

- требование об исключении или исправлении неверных или неполных Персональных данных, а также данных, обработанных с нарушением требований ТК РФ или иного федерального закона. При отказе Общества исключить или исправить Персональные данные Работника он имеет право заявить в письменной форме Обществу о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;
- требование об извещении Обществом всех лиц, которым ранее были сообщены неверные или неполные Персональные данные Работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжалование в суд любых неправомерных действий или бездействия Общества при обработке и защите его Персональных данных.

13.2. В соответствии с положениями Федерального закона Работник имеет право на получение информации, касающейся обработки его Персональных данных, в том числе содержащей:

- подтверждение факта обработки Персональных данных Обществом;
- правовые основания и цели обработки Персональных данных;
- цели и применяемые Обществом способы обработки Персональных данных;
- наименование и место нахождения Общества, сведения о лицах (за исключением Работников Общества), которые имеют доступ к Персональным данным или которым могут быть раскрыты Персональные данные на основании договора с Обществом или на основании Федерального закона;
- обрабатываемые Персональные данные, относящиеся к соответствующему Работнику, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом;
- сроки обработки Персональных данных, в том числе сроки их хранения;
- порядок осуществления Работником прав, предусмотренных Федеральным законом;
- информацию об осуществленной или о предполагаемой трансграничной передаче Персональных данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку Персональных данных по поручению Общества, если обработка поручена или будет поручена такому лицу;
- информацию о способах исполнения Обществом установленных мер, направленных на обеспечение выполнения Обществом обязанностей, предусмотренных Федеральным законом;
- иные сведения, предусмотренные Федеральным законом или другими федеральными законами.

13.2.1. Сведения, указанные в п. 13.2. настоящей Политики, должны быть предоставлены Работнику Обществом в доступной форме, и в них не должны содержаться Персональные данные, относящиеся к другим Работникам, за исключением случаев, если имеются законные основания для раскрытия таких Персональных данных.

13.2.1. Сведения указанные в п. 13.2. настоящей Политики предоставляются Работнику или его законному представителю Обществом в течение *десяти рабочих дней* с момента обращения либо получения Обществом запроса Работника или его законного представителя.

Указанный срок может быть продлен, но не более чем на *пять рабочих дней* в случае направления Обществом в адрес Работника мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

13.2.2. Запрос должен содержать:

- номер основного документа, удостоверяющего личность Работника или его законного представителя;
- сведения о дате выдачи указанного документа и выдавшем его органе;
- сведения, подтверждающие участие Работника в отношениях с Обществом (номер договора, дата заключения договора, либо сведения, иным образом подтверждающие факт обработки Персональных данных Обществом);
- подпись Работника или его законного представителя.

13.2.3. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации. Общество предоставляет сведения, указанные в п. 13.2 настоящей Политики Работнику или его

законному представителю в той форме, в которой направлены соответствующие обращение либо запрос, если иное не указано в обращении или запросе.

13.2.4. Работник вправе требовать от Общества уточнения его Персональных данных, их блокирования или уничтожения в случае, если Персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

13.3. Право на обжалование действий или бездействия Общества.

13.3.1. Если работник данных считает, что Общество осуществляет обработку его Персональных данных с нарушением требований настоящего Федерального закона или иным образом нарушает его права и свободы, Работник вправе обжаловать действия или бездействие Общества в уполномоченный орган по защите прав субъектов Персональных данных или в судебном порядке.

13.3.2. Работник имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

13.4. Работник обязан:

- предоставлять Обществу только достоверные свои Персональных данных, входящие в перечень, утверждённый Руководителем;
- своевременно сообщать Обществу об изменении своих Персональных данных;
- быть ознакомленным под подпись с организационно-регламентирующей документацией и нормативно-локальными актами Общества в области обработки и защиты Персональных данных, также об их правах и обязанностях в этой области;
- Работник не должен отказываться от своих прав на сохранение и защиту тайны.

13.5. Право Работника на доступ к его Персональных данных может быть ограничено в соответствии с ч. 8 ст. 14 Федерального закона.

14. ОБЯЗАННОСТИ И ПРАВА ОБЩЕСТВА

С целью выполнения обязанностей, предусмотренных Федеральным законом, Общество в соответствии с юридическими, организационными и техническими мерами обязано:

14.1. Обязанности Общества при сборе Персональных данных:

14.1.1. При сборе Персональных данных Общество обязано предоставить Работнику по его просьбе информацию, предусмотренную п. 13.2. настоящей Политики.

14.1.2. Если в соответствии с Федеральным законом предоставление Персональных данных и (или) получение Обществом Согласия являются обязательными, Общество обязано разъяснить Работнику юридические последствия отказа предоставить его Персональные данные и (или) дать Согласие на их обработку.

14.1.3. При сборе Персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», Общество обязано обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение Персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации за исключением случаев, указанных в Федеральном законе.

14.2. Меры, направленные на обеспечение выполнения Обществом обязанностей, предусмотренных Федеральным законом.

14.2.1. Общество обязано принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами. Общество самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено настоящим Федеральным законом или другими федеральными законами. К таким мерам, в частности, относятся:

- назначение Обществом ответственного за организацию обработки Персональных данных;
- издание Обществом документов, определяющих Политику Общества в отношении обработки Персональных данных, локальных актов по вопросам обработки Персональных данных, определяющих для каждой цели обработки Персональных данных:
  - категории и перечень обрабатываемых Персональных данных;
  - способы, сроки обработки и хранения Персональных данных;

- порядок уничтожения Персональных данных при достижении целей их обработки или при наступлении иных законных оснований, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений. Такие документы и локальные акты не могут содержать положения, ограничивающие права Работников, а также возлагающие на Общество не предусмотренные законодательством Российской Федерации полномочия и обязанности;

- применение правовых, организационных и технических мер по обеспечению безопасности Персональных данных в соответствии со ст. 19 Федерального закона;
- осуществление внутреннего контроля и (или) аудита соответствия обработки Персональных данных Федеральному закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите Персональных данных, Политике Общества, локальным актам Общества;
- оценка вреда в соответствии с требованиями, установленными уполномоченным органом по защите прав субъектов персональных данных, который может быть причинен Работникам в случае нарушения настоящего Федерального закона, соотношение указанного вреда и принимаемых Обществом мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом;
- ознакомление сотрудников Общества, непосредственно осуществляющих обработку Персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите Персональных данных, документами, определяющими Политику, локальными актами по вопросам обработки Персональных данных, и (или) обучение указанных сотрудников.

14.2.2. Общество обязано опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его Политику, к сведениям о реализуемых требованиях к защите Персональных данных.

14.2.3. Общество обязано представить документы и локальные акты, указанные в п. 14.2.1. настоящей Политики, и (или) иным образом подтвердить принятие мер, указанных в п. 14.2.1. настоящей Политики, по запросу уполномоченного органа по защите прав субъектов персональных данных.

14.3. Меры по обеспечению безопасности Персональных данных при их обработке.

14.3.1. Общество при обработке Персональных данных обязано 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 Персональных данных.

14.3.2. Обеспечение безопасности Персональных данных достигается, в частности:

- определением угроз безопасности Персональных данных при их обработке в ИСПДн;
- применением организационных и технических мер по обеспечению безопасности Персональных данных при их обработке в ИСПДн, необходимых для выполнения требований к защите Персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности Персональных данных;
- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации (далее – СЗИ);
- оценкой эффективности принимаемых мер по обеспечению безопасности Персональных данных до ввода в эксплуатацию ИСПДн;
- учетом машинных носителей Персональных данных;
- обнаружением фактов несанкционированного доступа к Персональным данным и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на ИСПДн и по реагированию на компьютерные инциденты в них;
- восстановлением Персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установлением правил доступа к Персональным данным, обрабатываемым в ИСПДн, а также обеспечением регистрации и учета всех действий, совершаемых с Персональными данными в ИСПДн;
- контролем за принимаемыми мерами по обеспечению безопасности Персональных данных и уровня защищенности ИСПДн.

14.3.3. Общество обязано соблюдать требования, установленные Правительством Российской Федерации с учетом возможного вреда Работнику, объема и содержания обрабатываемых Персональных данных, вида деятельности, при осуществлении которого обрабатываются Персональные данные, актуальности угроз безопасности Персональных данных в соответствии с ч. 3 ст. 19 Федерального закона.

14.3.4. Общество обязано использовать и хранить биометрические Персональные данные вне ИСПДн только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения.

14.3.5. Общество обязано 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.

14.4. Обязанности Общества при обращении к нему Работника либо при получении запроса Работника или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных.

14.4.1. При обращении Работника либо при получении запроса Работника или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных действия Общества в обязательном порядке регламентируются в соответствии со ст. 20 Федерального закона.

14.5. Обязанности Общества по устранению нарушений законодательства, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению Персональных данных.

14.5.1. По устранению нарушений законодательства, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению Персональных данных действия Общества в обязательном порядке регламентируются в соответствии со ст. 21 Федерального закона.

14.6. Уведомление об обработке Персональных данных

14.6.1. Общество до начала обработки Персональных данных обязано уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку Персональных данных, за исключением случаев, предусмотренных ч. 2 ст. 22 Федерального закона.

14.6.2. Действия Общества, связанные с уведомлением уполномоченного органа по защите прав субъектов персональных данных, в обязательном порядке регламентируются в соответствии со ст. 22 Федерального закона.

14.7. Обязанности лица, ответственного за организацию обработки Персональных данных в Обществе.

14.7.1. Общество, являющееся юридическим лицом, назначает лицо, ответственное за организацию обработки Персональных данных.

14.7.2. Лицо, ответственное за организацию обработки Персональных данных, получает указания непосредственно от Руководителя и подотчетно ему.

14.7.3. Общество обязано предоставлять лицу, ответственному за организацию обработки Персональных данных, сведения, указанные в ч. 3 ст. 22 Федерального закона.

14.7.4. Лицо, ответственное за организацию обработки Персональных данных, в частности, обязано:

- осуществлять внутренний контроль за соблюдением Обществом и его Работниками законодательства Российской Федерации о Персональных данных, в том числе требований к защите Персональных данных;
- доводить до сведения Работников Общества положения законодательства Российской Федерации о Персональных данных, локальных актов по вопросам обработки Персональных данных, требований к защите Персональных данных;
- организовывать прием и обработку обращений и запросов Работников или их законных представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

14.7.5. Иные права, обязанности и действия должностных лиц, в трудовые обязанности которых входит обработка Персональных данных, определяются их должностными инструкциями.

15. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ И НАРУШЕНИЕ ТРЕБОВАНИЙ ФЕДЕРАЛЬНОГО ЗАКОНА

15.1. В соответствии со ст. 90 ТК РФ лица, виновные в нарушении положений законодательства Российской Федерации в области персональных данных при обработке Персональных данных Работника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном настоящим Кодексом и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

15.2. В соответствии со ст. 24 Федерального закона:

15.2.1. Лица, виновные в нарушении требований Федерального закона, несут предусмотренную законодательством Российской Федерации ответственность.

15.2.2. Моральный вред, причиненный Работнику вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных Федеральным законом, а также требований к защите Персональных данных, установленных в соответствии с Федеральным законом, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных Работником убытков.

16. ПОРЯДОК АКТУАЛИЗАЦИЯ И УТВЕРЖДЕНИЯ ПОЛИТИКИ

16.1. Политика утверждается и вводится в действие приказом Руководителя Общества.

16.2. Настоящая Политика подлежит актуализации периодически, но не чаще, чем один раз в год, а также в следующих случаях:

- при изменении законодательства Российской Федерации в области обработки и защиты персональных данных;
- при изменении целей обработки Персональных данных, структуры информационных и/или телекоммуникационных систем (или введении новых);
- при применении новых технологий обработки Персональных данных;
- при появлении необходимости в изменении процесса обработки Персональных данных, связанной с деятельностью Общества;
- по результатам контроля выполнения требований по обработке и защите Персональных данных;
- при изменении локальных нормативных актов Общества, регламентирующих организацию обработки и обеспечение безопасности Персональных данных.

16.3. При внесении изменений в заголовке Политики указывается дата последнего обновления редакции. Новая редакция Политики вступает в силу с момента ее утверждения, если иное не предусмотрено новой редакцией Политики.

16.4. Политика содержит сведения, подлежащие раскрытию, является общедоступным документом Общества и предусматривает возможность ознакомления с ней любых лиц.

16.5. Актуальная версия Политики опубликована на сайте Общества https://kgilc.ru и вступает в силу с момента её размещения.

Разработал

Начальник службы безопасности _____ А.И. Романихин

Согласовано

Юридический отдел _____ Н.Г. Демидова

Отдел кадров _____ Г.Н. Викуловская